TRABAJO FIN DE MÁSTER

Escuela Técnica Superior de Ingenieros Informáticos
Universidad Politécnica de Madrid

Secretify - De la idea al mercado

Urko Alberto Martinez Cirez
Director: Juan Carlos Crespo Zaragoza

Agradecimientos

Muchas gracias.

Mi más enorme agradecimiento va a los míos, a los que están aquí y a los que están más lejos, quienes me han hecho ser como soy, espero que estén orgullos de mí, estén donde estén.

Por supuesto, a ella. Te debo otras vacaciones. L.

Muchas gracias a los que me han permitido acabar este Trabajo, quitando tiempo de otros menesteres.

Resumen

La extrema competitividad derivada de la globalización, hace que los proyectos en Tecnologías de la Información (TI), no se valoren por si son buenos o malos. Se da por supuesto que el producto tecnológico es innovador, aporta un valor añadido y tiene un fundamento tecnológico sólido y bien construido.

Europa es un gran exponente en Desarrollo e Investigación (I+D), pero todavía está por detrás de países como Estados Unidos o Japón en cuanto a Innovación (i). Nos falta conseguir llegar al mercado. No basta con conseguir con éxito una prueba de concepto. Hay que ir más allá.

Partimos de la base de un proyecto: Secretify, un cliente de correo web multicuenta sencillo y atractivo que permite a los usuarios cifrar sus comunicaciones utilizando cuentas de correo electrónico ya existentes, sin la necesidad de saber nada sobre seguridad, criptografía o gestión de claves.

La finalidad de este Trabajo es aplicar todos los conceptos aprendidos durante el Máster (en concreto en la rama de Gestión, Innovación y Negocio TI), para convertir Secretify en un producto que sacar al mercado con éxito, teniendo los conocimientos tanto técnicos como empresariales, para minimizar los riesgos y adecuarse al mercado.

Palabras clave

Seguridad, Negocio TI, Emprendimiento, Innovación.

Abstract

The extreme competitiveness derived from globalization, makes projects in Information Technologies (IT) to not be evaluated for its goodness. It is assumed that the technology product is innovative, provides added value and has a solid technology basis and well constructed.

Europe is a great exponent in Research & Development (R&D), but It is still far behind from countries like USA or Japan in terms of Innovation (i). We need to reach the market: it is not enough having a successful proof of concept. We must go further.

We start from a project: Secretify, a simple and beautiful web-based multiaccount email client that allow users to cypher their communications using already existing email accounts, without the need to know about security, cryptography or key management.

The purpose of this thesis is to apply all concepts learnt during the Master course (specifically in Management, Innovation and IT business), to turn Secretify into a successful market launch, having the technical and business knowledges, in order to reduce the risks and to adapt to the market.

Key words

Security, IT Business, Entrepreneurship, Innovation.

Índice de contenidos

Listado de figuras

Listado de tablas

Capítulo 1. Introducción

1.1. Introducción

El presente trabajo pretende convertir un proyecto tecnológico en un producto comercial, poniendo la lupa en aspectos no tan técnicos sino más de negocios, bajo el paraguas de la intensificación en "Gestión, Innovación y Negocio TI", del Máster Universitario en Ingeniería Informática (MUII), cuyo Trabajo de Fin de Máster tiene el lector delante.

Este Trabajo parte de la base de "Desarrollo de un cliente web de emails seguros; Secretify", Trabajo Final de Máster de Esaú Suárez Ramos, en la Universitat Oberta de Catalunya (http://hdl.handle.net/10609/35401).

Esaú Suárez y Urko Martinez, autor del presente Trabajo son amigos y socios de una empresa de base tecnológica, Guayota Studios, con la que van a comercializar un servicio de correo electrónico seguro, a partir de ambos trabajos.

1.2. Contexto

La Revolución Industrial supuso el cambio de una era: del trabajo individual y artesanal, se pasó a las grandes fábricas mecanizadas; del carro de tiro, al ferrocarril; de los barcos de vela, a los de vapor.

El mundo cambió en unas pocas décadas. Y no sólo fueron cambios económicos, sino también demográficos y sociales. La gente migró desde las zonas rurales a las urbanas. Se empezaron a perfilar las grandes ciudades. Con las colosales fábricas y sus producciones en serie, el desarrollo del capitalismo más egoísta y avaricioso dio lugar a las grandes desigualdades entre clases.

Las diferencias entre pobres y ricos se acentuaron sobremanera. La riqueza y pompa con la que vivían los grandes propietarios y burgueses contrastaba con la pobreza desmedida de la clase trabajadora, el proletariado, que deriva del latín *proletarii*, los que

crían hijos. Su única función, casi como en la Antigua Roma, era la de criar hijos, los cuales debían seguir los pasos de sus padres y trabajar de sol a sol por un mísero jornal.

Estas desigualdades dieron lugar a los movimientos obreros, empujaron al liberalismo frente al conservadurismo y abrieron un camino sin retorno: el progreso.

La caída del Antiguo Régimen, la Ilustración, la revolución liberal y la Independencia de los Estados Unidos de América, dieron a luz en Europa a la Revolución Francesa.

Todos estos cambios, necesarios para llegar a la sociedad actual en la que vivimos, fueron de tal importancia que incluso tiene un nombre. Pasamos de la Edad Moderna a la Contemporánea.

¿Por qué hablar de Historia? Porque la Revolución Industrial fue la primera ficha de dominó que cayó sobre el tablero del Mundo. Los cambios económicos dieron paso a los cambios sociales. Los cambios sociales dieron la vuelta al mundo y permitieron el desarrollo de una clase media.

Ahora estamos en una nueva Revolución Industrial, la Revolución Digital. Como entonces, las diferencias entre ricos y pobres se ha agudizado, la clase media, que tanto costó conseguir, se tambalea, y el Estado del Bienestar hace aguas.

Los modelos económicos cambian. Y las Tecnologías de la Información y las Comunicaciones (TIC), tienen un papel importante.

El desarrollo de la Informática, no sólo permite hacer más y mejores cosas, sino que ahora son accesibles a cualquiera. En los años 60, se necesitaban salas enteras para almacenar uno de aquellos primeros ordenadores. Ahora llevamos dispositivos electrónicos en nuestros bolsillos infinitamente más potentes que aquellos.

La popularización de los equipos informáticos, el desarrollo de Internet actual, y la cantidad y calidad de los contenidos que se pueden encontrar, de forma gratuita o pagando, hace que cualquiera, desde su casa, pueda aprender, desde programación a física o matemáticas.

Las aplicaciones han sido, desde el inicio de la informática o la computación, el alma de los ordenadores. En un principio, las aplicaciones informáticas dependían de la plataforma (no eran intercambiables y estaban sujetas a las restricciones de su sistema). A continuación, se popularizaron las aplicaciones independientes de plataforma, o portables. Actualmente, gracias al desarrollo de ecosistemas como el *cloud computing*, vivimos en el "boom" de las aplicaciones web y las aplicaciones móviles.

La gran adopción por parte del los consumidores de las últimas tecnologías, como los smartphones (la penetración del smartphone en España es del 81%, según la Fundación Telefónica [1]), y la popularidad de las *Apps*, las aplicaciones móviles, ha abierto un mercado floreciente, donde muchos particulares o pequeñas empresas han alcanzado niveles de ventas inimaginables.

Sin embargo, la última Crisis económica, nos demuestra los peligros de las burbujas económicas y especulativas, y nos empuja hacia una economía y una sociedad más sostenible y concienciada.

Entre otras cosas, la sociedad actual, llamada de la información, empieza a ser consciente de los problemas y peligros que entraña la Red. Y decimos empieza a ser, porque, a diferencia de lo que ocurre en nuestra vida habitual, la vida física, terrenal, "no digital", la cual está plagada de peligros que conocemos y enfrentamos, en Internet, la mayoría de usuarios no es del todo consciente de los peligros que atañen a la Red de redes.

Cuando hablamos de Seguridad en la Información, estamos haciendo referencia a diferentes propiedades, entre las que están la Confidencialidad, la Integridad o la Disponibilidad de la información.

La confidencialidad es un aspecto esencial para la protección de la privacidad de las personas, en concreto en la protección de la privacidad de las comunicaciones. La mayor parte de las empresas e instituciones tienen en su poder una gran cantidad de información sensible o confidencial, que merece una protección.

Por otro lado, las organizaciones manejan datos personales o privados, que van desde una simple dirección de correo electrónico, hasta los datos médicos de un paciente o su

1. Informe Sociedad de la Información en España 2014. 2015. VV.AA. Fundación Telefónica.

tendencia sexual. La Ley Orgánica de Protección de Datos (LOPD), hace especial referencia a la información personal más sensible que obliga a proteger, regulando los requisitos mínimos de seguridad que se deben aplicar. A pesar de ello, muchas veces no se hace, ya sea por ignorancia o por omisión voluntaria.

En cualquier caso, es fundamental incentivar la seguridad y mejorar la privacidad de las personas y sus comunicaciones, tanto en el ámbito público como en el privado. Y es menester de los profesionales de la Informática, y en concreto de los de la Seguridad de la Información, el facilitar los mecanismos necesarios para que se haga de forma sencilla y asequible.

Y es que, en el segundo decenio del siglo XXI, mientras desarrollamos conceptos y paradigmas innovadores y disruptivos, mientras tratamos de saltar de la web 3.0 al Internet de las Cosas, mientras desarrollamos sistemas capaces de procesar y analizar conjuntos masivos de datos no estructurados de forma automática, mientras todo eso ocurre, nos estamos olvidando de las personas como individuos.

El emprendimiento tecnológico, que tiene su cuna y máximo exponente de representación en Silicon Valley, California, ha dado lugar a un desarrollo espectacular en unas pocas décadas, haciendo de las empresas tecnológicas las que más cotizan en los mercados bursátiles internacionales.

Este atractivo económico, unido al auge del emprendimiento como respuesta a la falta o poca calidad del empleo actual, en especial en España, así como una inversión inicial relativamente baja, en comparación con los negocios tradicionales, ha hecho que muchas personas se atrevan a montar un negocio tecnológico o en Internet.

En muchas ocasiones, estos emprendedores no gozan de una experiencia o un conocimiento suficiente como para enfrentarse a los desafíos que supone el emprendimiento; y es por ello que, entre otros motivos, el 90% de las startups fracasan [2].

Por otro lado, tenemos que la mayoría de los servicios que se ofrecen por internet tienen un coste cero: son gratis. Un ejemplo de esto es toda la suite de aplicaciones de Google, que incluye Gmail, Inbox, Drive, Maps o Calendar, entre otros. Este tipo de “prácticas”

2. Why startups fail, according to their founders. http://fortune.com/2014/09/25/why-startups-fail-according-to-their-founders/

ha hecho que la mentalidad del usuario actual de internet vea como algo normal no tener que pagar nada por un servicio en la red. Si esto lo aplicamos a un caso particular, como es el de los proveedores de correo electrónico, vemos que los más comunes, que son Gmail, Outlook (antes Hotmail), Yahoo! Mail o Mail.com, ofrecen cuentas de correo totalmente gratuitas con, en algunos casos, almacenaje de emails ilimitado.

Aunque se trate de un servicio en internet, lo cual puede reducir costes de forma significativa frente a un negocio tradicional o físico, este tipo de servicios masivos gratuitos necesitan una infraestructura muy potente, lo que se traduce en grandes centros de procesamiento de datos (CPD), grandes consumos energéticos y personal especializado para tareas de mantenimiento y gestión. Si, en vez de tener estos CPD en propiedad, evitan esta gran inversión (CAPEX), y pasan esos gastos a operación (OPEX), nos encontraríamos igualmente con que tienen que hacer frente a unos gastos enormes de forma recurrente. Entonces, ¿cómo se logra mantener servicios que conllevan un gran coste por el cual no se recibe un ingreso por parte del usuario?

La respuesta es “sencilla”: se saca dinero de otra parte, pero se saca.

Entonces, tenemos que para estos servicios “gratuitos”, los usuarios realmente no son sus clientes, sino meros usuarios o terceros. Sus clientes (quienes pagan), son las empresas que están interesadas en los datos y la información que los usuarios están generando. Así, la mayoría de los usuarios se convierten en un producto, y al igual que un producto normal, se venden.

Esta reflexión, que nosotros hemos realizado siguiendo una lógica bastante sencilla en unas pocas líneas, y la facilidad con la que los usuarios han aceptado e incluso han dado la bienvenida con los brazos abiertos a este tipo de prácticas, a cambio de tener servicios gratuitos, aún perdiendo (de forma consciente o no), el control de cierta parte de la información personal y privada, es alarmante.

A día de hoy, no somos conscientes del daño que se le está haciendo a la privacidad de los individuos. Lo que nos puede parecer curioso, e incluso divertido, como es que nos aparezca en los anuncios de las webs que visitamos, casualmente, un producto que hemos buscado en Google, es un primer paso para que las empresas de este tipo sepan qué es lo que vamos a querer comprar, incluso antes de saberlo nosotros mismos.

Sin embargo, parece que la conciencia está cambiando. Nos damos cuenta de que no hay nada gratis y, en especial las empresas que gestionan y manejan datos sensibles y confidenciales, ven cada vez más la importancia de proteger el activo más valioso de las organizaciones de nuestros días: su información.

Así pues, parece evidente que es deseable, e incluso necesario, formar en aspectos de innovación, emprendimiento y negocio a los potenciales emprendedores, para tratar de evitar que caigan en las malas prácticas y los errores de sus predecesores; así como un estudio y una conciencia sobre la economía y la sociedad, en el sentido más general, para promover una forma de hacer negocios sostenible, apoyando de alguna manera el desarrollo y la protección de los derechos de las personas.

La introducción de servicios y productos en internet que a la vez sean asequibles y respetuosos con la privacidad, es un fenómeno muy deseable en nuestra sociedad, puesto que incluso aumentaría la percepción del valor de las aplicaciones de internet en general. Este tipo de servicios pueden convivir perfectamente con los actuales servicios gratuitos, siempre y cuando el usuario sea consciente de hasta dónde cede sus datos.

1.3. Antecedentes y Estado del Arte

Si dejamos una cartera repleta de dinero en la calle o si nos vamos de vacaciones y no cerramos la puerta de nuestra casa, no nos sorprendería quedamos sin ese dinero o si nos avisan de que alguien ha entrado en nuestra casa mientras no estábamos.

De la misma forma, si no protegemos nuestros sistemas en internet, no nos debemos sorprender si alguien intenta acceder a ellos, apropiarse de la información que almacenamos o nos deja un mensaje para hacernos saber que ha entrado.

La seguridad aplicada a los sistemas informáticos es necesaria, de la misma forma que lo es en la vida real. Sin embargo, al igual que ocurre en ésta, no existe ningún sistema 100% seguro. Quizás, la única excepción a esto, y con algunas reservas, nos la da uno de los mayores referentes mundiales en seguridad informática, Gene Spafford: "*The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards - and even then I have my doubts.*". Esto es, un sistema apagado en el interior de un bloque de hormigón en una habitación sellada protegida por guardias, y aún así, tiene sus dudas.

Aún a pesar de no disponer de sistemas que garanticen un 100% de seguridad, existen procedimientos, protocolos y aplicativos que permiten proteger estos sistemas, lo que permite mitigar la mayoría de los ataques o intentos de acceso no autorizados.

Un ámbito sensible de la Seguridad de la Información, es el de la protección de la Intimidad y la Privacidad de las personas. Dentro de este ámbito, se incluye la protección de los datos de carácter personal (desde número de teléfono, datos identificativos, tendencia sexual o credo), y la privacidad de las comunicaciones.

El derecho a la privacidad de las comunicaciones es un derecho recogido en la Declaración Universal de los Derechos Humanos, en su artículo 12, que dice: *"Nadie será objeto de interferencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra ni a su reputación. Toda persona tiene derecho a la protección de la ley contra tales interferencias o ataques."*

Además en la Constitución Española de 1978, Art. 18, tenemos que:
"1. Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en el sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.
3. Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.
4. La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos."

Como vemos, la protección de las comunicaciones es un derecho internacionalmente reconocido, estando los ataques al mismo penados por la ley.

Pongámonos en el supuesto de que, al llegar a nuestro domicilio particular, nos encontramos con que las cartas a nuestro nombre han sido abiertas y leídas. Puede que, en el caso de alguna comunicación comercial, no nos moleste más allá del hecho de que nos hayan abierto un sobre que iba a nuestro nombre; pero si se produce el caso de que nos han abierto una carta con información que consideramos importante (datos bancarios, comunicaciones con seres queridos o de un partido político), es lógica la reacción de avisar a las autoridades y poner las denuncias pertinentes.

Más aún, si sabemos quién ha violado la intimidad de dichas comunicaciones, seguramente tomaríamos medidas legales contra esta persona o grupo de personas.

Sin embargo, parece que nuestra vida en Internet es diferente a nuestra vida "terrenal".

Todos los días, cada vez que recibimos un email a través de los múltiples proveedores de correo electrónico que nos ofrecen el servicio de forma gratuita, nuestras comunicaciones son sistemáticamente monitorizadas en busca de palabras clave que se utilizan para crear un perfil de usuario al cual poder enviar publicidad dirigida.

Esto, desde un punto de vista comercial, es beneficioso tanto para el proveedor como para el usuario. Para este, porque recibe publicidad de productos y servicios en los cuales puede estar interesado (y puestos a recibir publicidad, mejor que me interese); para aquél, puede ofrecer a terceras empresas mostrar publicidad a potenciales clientes, no dando palos de ciego (lo que, presumiblemente, aumentará la conversión y se optimizará el pago por click).

No obstante, si nos vamos a un plano más, llamémoslo, filosófico, detrás de esta interesante acción de marketing/comercial, subyace una flagrante violación de la intimidad y el derecho a la privacidad del propietario de las comunicaciones.

¿Y es esto legal? Si nos fijamos en las legislaciones vigentes, no debería serlo. Sin embargo, nosotros como usuarios aceptamos una serie de términos y condiciones en las que se da a entender que puede que este tipo de acciones se realicen. Así pues, al aceptar estos términos y condiciones, estamos autorizando y legitimando la acción.

¿Nos están engañando? Realmente, no. Si no leemos las condiciones en las que se nos va a prestar el servicio, el problema es nuestro. Si lo leemos y lo aceptamos, estamos reconociendo qué hace cada parte en el asunto, y no deberíamos esperar mucho respeto por la privacidad de esas comunicaciones.

Y ésta última afirmación viene acorde a los comentarios por parte de Google, cuando se les inquirió sobre este tema en 2013 [3]: *"Los usuarios de servicios de correo electrónico basado en la web realmente no deberían sorprenderse si sus correos son*

3. Google: don't expect privacy when sending to Gmail. The Guardian. http://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit

procesados por el proveedor del servicio. Es la misma situación del remitente de una carta a través de correo tradicional, que no debe sorprenderse si el servicio postal la abre y revisa su contenido. Una persona realmente no tiene expectativas de privacidad absoluta en la información que ofrece a terceros de manera voluntaria".

Es más, a pesar de la legislación vigente en Europa y en concreto, en España, sobre la protección de las comunicaciones, existe otro tipo de legislación que se escuda en la lucha contra el terrorismo y otros crímenes graves, como es la conocida como *Patriot Act* [4] estadounidense, que obliga a los grandes proveedores de contenido a almacenar, durante un tiempo indeterminado, la información que pasa por sus servidores. Y esto incluye la información relativa a los correos electrónicos.

¿Puede que se estén recortando los derechos y las libertades de los ciudadanos en nombre de la protección frente al terrorismo? ¿Puede que este tipo de actividades puedan ser, no ya un ataque contra un derecho fundamental recogido en la constitución, sino un potencial peligro contra nuestro sistema democrático? ¿Dónde está la línea entre la protección y la seguridad del Estado y las libertades y derechos individuales de los ciudadanos? No tenemos una respuesta a eso. El Tribunal Europeo de Derechos Humanos (TEDH), advierte que hay que establecer "garantías suficientes contra los abusos, ya que un sistema de vigilancia secreta destinado a proteger la seguridad nacional crea el riesgo de minar, o incluso destruir, la democracia pretendiendo defenderla" [5].

Entonces, ¿hay alguna alternativa?

En cuanto al correo electrónico, el problema principal es que estos proveedores tienen acceso al contenido de los mensajes. ¿La solución? Simplemente, no permitiéndoles acceder al contenido. ¿Cómo? Cifrando el contenido.

Sin embargo, gestionar el cifrado de mensajes no es un asunto trivial, ni desde el punto de vista tecnológico, ni desde el punto de vista de la regulación competente.

Uno de los servicios de correo electrónico cifrado que más éxito tuvo, fue Lavabit, con 410.000 usuarios, que fue obligado a cerrar, supuestamente, por presiones gubernamentales [6], cuyo usuario más conocido fue Edward Snowden, consultor

4. Patriot Act. Wikipedia. http://en.wikipedia.org/wiki/Patriot_Act
5. Sentencia del TEDH Klass y otros contra Alemania, 1978, y Sentencia del TEDH Leander contra Suecia, 1987. Cita de Rodríguez, O. T. (2014). Seguridad del Estado y privacidad. Editorial Reus.
6. Secrets, lies and Snowden's email: why I was forced to shut down Lavabit. The Guardian. http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email

externo de la Agencia de Seguridad Nacional estadounidense (NSA), célebre por revelar la existencia de programas de vigilancia masiva a nivel mundial.

Los motivos reales del cese de la actividad de Lavabit todavía son un enigma, pero en una carta que firmaba su fundador, Ladar Levison, en su web (http://lavabit.com/), dice que se opuso a entregar las "claves privadas de cifrado de la empresa", puesto que esto daba acceso a descifrar el contenido de los mensajes de la plataforma. Lo que realmente se le estaba requiriendo, era poder acceder a todos los mensajes de todos lo usuarios del servicio, por lo que éste no tenía sentido. Según sus palabras, tuvo que elegir entre "convertirse en cómplice de crímenes contra el pueblo estadounidense o dejar casi 10 años de duro trabajo y cerrar Lavabit".

A pesar del cierre de Lavabit, actualmente existen diferentes aproximaciones de correo electrónico cifrado.

Por un lado, tenemos extensiones o plugins para navegadores de internet (como Chrome o Firefox). Estos detectarían cuando vamos a enviar un email con los proveedores de email que soporten, y presentarían las opciones de cifrado o firma. Como ejemplos, tenemos a Mailvelope, que permite cifrar correos de Gmail o de Yahoo! Mail si utilizamos el navegador de Google Chrome o de Mozilla Firefox; y tenemos SafeGmail, que se instala en Chrome y sirve para cifrar exclusivamente los correos Gmail. Esta aproximación cuenta con una limitación importante en cuanto a los proveedores de correo electrónico y los navegadores donde se instala.

Por otro lado, tenemos los complementos a clientes de correo electrónico [7] (como Mozilla Thunderbird, Apple Mail o Microsoft Outlook), que añaden las funcionalidades de cifrado y seguridad, que generalmente no se incluyen. Un ejemplo es EnigMail. Estos complementos arrastran la desventaja del medio donde se instalan: son exclusivos de los clientes de correo, los cuales son dependientes del sistema. Además, los complementos y las extensiones no suelen incluir una gestión sencilla de las claves propias y de contactos.

Frente a estas alternativas, tenemos servicios más parecidos a Lavabit. Constan de un cliente web de correo electrónico (accesible, por tanto, desde cualquier navegador, independientemente del sistema). En la mayoría de los casos se utilizan sistemas de

7. Cliente de correo electrónico. Wikipedia. http://es.wikipedia.org/wiki/Cliente_de_correo_electr%C3%B3nico

cifrado bastante robustos, pero se suele obligar a crear una nueva cuenta de correo electrónico, no dan excesivas facilidades de uso y cuentas con una interfaz de usuario algo anticuada. Vamos a ver con algo más de profundidad algunos servicios:

- Hushmail

Este servicio, lanzado en 1999, ofrece para particulares una versión gratuita y dos de pago. En todas estas versiones, se tiene que crear una nueva cuenta de correo de la forma nombre@hushmail.com, y se diferencian entre sí en los límites de almacenamiento que establecen y la forma de acceso. Los precios van desde 34,99 a los 49,98 $ (USD) al año.

Por otro lado, ofrece un servicio para empresas, con un coste por usuario de 5,24 $ (USD) al mes, que permite utilizar el dominio personalizado de la empresa, de la forma nombre@empresa.com.

Tanto para particulares como para empresas ofrece un sistema robusto de cifrado, aplicando el esquema de OpenPGP.

- ProtonMail

Es un joven servicio de correo cifrado, que busca convertirse en el sustituto suizo de Lavabit. Desarrollado por jóvenes investigadores del CERN y estudiantes del MIT, se posiciona como un servicio de cifrado punto a punto web más moderno. Ofrece envío de email tanto a usuarios registrados como a no registrados. Los emails enviados a estos últimos, van protegidos por una contraseña proporcionado por el emisor del mensaje.

ProtonMail sólo se puede utilizar creando una cuenta nueva (usuario@protonmail.ch), y requiere dos contraseñas, una para iniciar sesión y otra para descifrar el buzón. Esto hace que no sea posible utilizar servicios de gestión de contraseñas, puesto que están pensados para una contraseña para una cuenta en concreto.

Actualmente están en fase beta gratuita. Quieren ofrecer un servicio básico gratuito de cifrado de correos, pero presumiblemente, se podrán ampliar los límites máximos de envío de mensajes y de capacidad de almacenamiento (storage), actualmente en 1.000 mensajes/mes y 500 MB.

En junio de 2014 lanzaron una campaña de crowdfunding en Indiegogo, con un objetivo de financiación mínimo de $100.000 (USD). Llegaron a recaudar, en un mes y medio, $550.377 (USD).

- DarkMail

La Dark Mail Technical Alliance, formada por Lavabit y Silent Circle (otra empresa que ofrece llamadas y mensajes de texto cifrados [8]), busca crear un protocolo y una arquitectura completa que permita el envío y la recepción de correo de forma privada y segura, tratando de esconder incluso los metadatos (remitente, destinatario, asunto, etc.), del mensaje. El proyecto comenzó en octubre de 2013, pero todavía no se ha publicado nada más allá de un documento de especificaciones y algo de código pre-alpha.

Como vemos, existen diferentes alternativas para el envío y la recepción de correos electrónicos cifrados. Sin embargo, dejan una serie de aspectos sin cubrir, lo que nos permite dar una solución tecnológica que se aproveche de ello.

1.4. Objetivos

A lo largo del presente documento se pretende dar una visión sobre los aspectos a tener en cuenta para lanzar un producto software al mercado, desde la idea inicial hasta el desarrollo de un plan de negocio con el que buscar financiación.

A continuación, se enumeran los objetivos específicos del Trabajo.

O1.- Definir el producto TI
O2.- Analizar y estudiar el mercado
O3.- Realizar un plan de comercialización del producto
O4.- Construir un plan de marketing
O5.- Desarrollar un plan de Internacionalización básico
O6.- Analizar gastos y elaborar cuadros financieros y previsiones
O7.- Elaborar un plan de negocio

8. Silent Circle. Wikipedia. http://en.wikipedia.org/wiki/Silent_Circle_(software)

Capítulo 2. La Idea

2.1. La idea original

Esta idea, como la mayoría de las ideas, surge de una necesidad: la necesidad de resolver un problema tecnológico, en un campo específico, que es la falta de privacidad en el correo electrónico.

El cifrado de correos existe casi desde el mismo momento en el que aparecen los correos. Se puede incluso cifrar correos electrónicos utilizando el conocido Microsoft Outlook. Sin embargo, el proceso de configuración y gestión de claves es tremendamente complejo, incluso para personas que están acostumbradas a trabajar con herramientas informáticas avanzadas.

En primer lugar, se debe obtener un certificado digital, ya sea adquiriéndolo de un tercero o autogenerando uno. Esto último se puede realizar utilizando herramientas como OpenSSL [9], lo cual no suele ser ni cómodo ni atractivo para usuarios que no tengan un perfil altamente técnico y estén habituados a trabajar con herramientas en línea de comandos o similar. Si se adquiere de un tercero, se puede incurrir en gastos procedentes de la emisión del certificado por una Autoridad Certificadora reconocida. Aunque se disponga del certificado digital de Persona Física emitido por la Fábrica Nacional de Moneda y Timbre, válido par el acceso con los recursos de la Administración Electrónica en España, no se podrá hacer uso del mismo para el asunto que nos interesa, puesto que en dicho certificado no se incluye mención alguna a la dirección de correo electrónico.

Llegados a este punto, cabe hacer una introducción de los principios de la criptografía asimétrica.

Básicamente y a diferencia de los sistemas de criptografía simétrica, se necesita de dos claves para cifrar y descifrar un mensaje. Esto es porque la clave de cifrado y la de descifrado son diferentes. ¿Cómo se aplica esto al envío de un mensaje entre Alicia y Bea? En primer lugar, todos los participantes en la comunicación deben disponer de dos

9. OpenSSL Project web. https://www.openssl.org/

claves: una clave pública (P) y una clave privada o secreta (S). Como su nombre indica, la clave pública de un usuario puede ser conocida por cualquier otro usuario, mientras que la privada debe ser de acceso único y exclusivo por parte de su propietario.

Acorde a este esquema, tenemos a Alicia con su clave pública (P_A), y su clave privada o secreta (S_A); y tenemos a Bea con su clave pública (P_B), y también con su clave secreta (S_B).

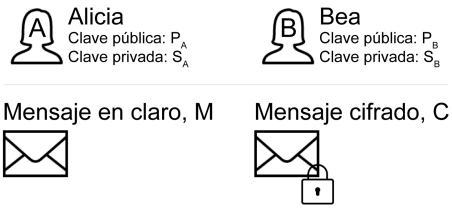

Figura 2.1. Notación del ejemplo de criptografía asimétrica.

Cuando Alicia quiere enviar un mensaje a Bea, el mensaje en claro (M), se cifra con la clave pública de Bea (P_B). El mensaje ya cifrado (C), es el que se remite a Bea por el canal que sea. Ésta, para descifrar el mensaje, debe aplicar su clave privada (S_B), sobre el mensaje cifrado (C), obteniendo como resultado el texto en claro (M).

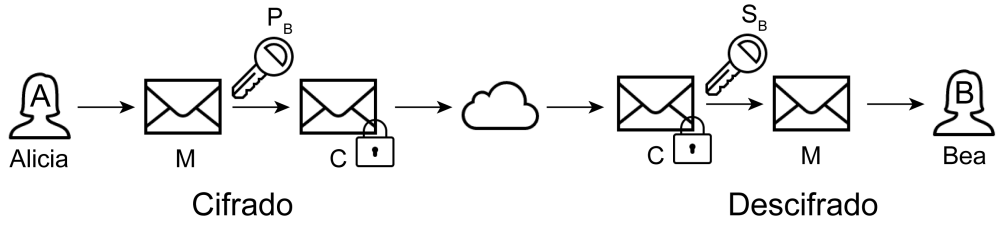

Figura 2.2. Esquema de cifrado y descifrado en criptografía asimétrica.

Como hemos visto en el ejemplo, si Alicia le quiere enviar un mensaje cifrado a Bea, necesita conocer previamente la clave pública de Bea.

Por tanto, en la práctica, suponiendo que remitente y destinatario tengan sendos certificados, la forma más sencilla para que Alicia reciba la clave pública de Bea es haciendo que Bea le envíe un mensaje firmado a Alicia, incluyendo su clave pública (P_B).

El proceso de firmado es el opuesto al de cifrado. Cuando Bea firma un mensaje, lo hace con su clave privada (S_B). Por tanto, para comprobar que la firma es realmente de Bea, se le aplica su clave pública (P_B).

Como vemos, este esquema no es sencillo ni cómodo de utilizar, se necesitan amplios conocimientos sobre criptografía y seguridad, para realizar el proceso de forma más o menos apropiada.

Este hecho no es extraño a las herramientas informáticas que añaden seguridad. En general, los profesionales de la informática, pensamos que el usuario tendrá un mínimo de conocimientos sobre el tema concreto, que se sentirá cómodo trabajando con interfaces de línea de comandos, y que es obvia la disposición y la función de cada uno de los elementos de interacción.

¿Qué es lo que estamos haciendo en realidad? Construir herramientas complejas e incluso desagradables a la vista, que hacen que los usuarios no técnicos vean la seguridad como un obstáculo que salvar, y no como algo deseable.

Entonces, ¿cual es la idea?

La idea es conseguir un sistema que permita proteger el correo electrónico, posibilitando enviar y recibir correo seguro, de una forma sencilla e intuitiva para cualquier persona, sin tener que crear nuevas cuentas de correo, y convertirlo en sinónimo de correo seguro.

En esencia, queremos mejorar la experiencia del usuario en el uso del correo electrónico, permitiendo añadir privacidad a sus comunicaciones con un click.

Nuestra máxima es: si eres capaz de enviar un correo electrónico, puedes enviarlo cifrado.

2.2. Solución tecnológica, de idea a proyecto

Encontrar la solución tecnológica que más se adecue a un problema es uno de los procesos más creativos, complejos y estimulantes que llevan a cabo los Ingenieros en Informática.

Teníamos entre manos una gran idea, habíamos logrado despertar interés en las personas cercanas, incluso algunos empezaban a ver cómo comercializarlo y crear una empresa de ello. Pero antes, tenemos que dar con la solución idónea, de entre todas las posibilidades.

En primer lugar, estudiamos las herramientas que actualmente existen, para tratar de detectar sus puntos fuertes y débiles, potenciando los primeros y corrigiendo los últimos.

Durante esta primera etapa se llevan a cabo una serie de entrevistas informales, con el fin de identificar y destacar los requisitos más importantes.

El nombre en clave que se escoge para el proyecto es Secretify o secretify.it.

2.2.1. Requisitos funcionales

Básicamente, queremos un sistema con el que poder enviar y recibir correo electrónico cifrado, de forma sencilla e intuitiva. ¿En qué se traduce esto?

Por un lado, el usuario necesita un cliente de email con el que poder gestionar su correo electrónico, independientemente de si está cifrado o no. En este caso, existen diferentes aproximaciones: trabajar sobre clientes ya existentes (Thunderbird, Outlook, etc), desarrollar un cliente nativo (instalable), desarrollar una aplicación web y/o desarrollar aplicaciones móviles.

Secretify debe poder trabajar sobre cuentas de correo electrónico ya existentes, sean estas de Gmail, Outlook/Hotmail, o de una organización en particular (por ejemplo, cuenta@upm.es). Además, se debe permitir tener varias cuentas configuradas simultáneamente.

Es deseable, para añadir más valor al cliente de correo, desarrollar funcionalidades avanzadas como la revocación de mensajes (esto es que se puede inhabilitar a un destinatario el acceso a un determinado mensaje), el envío de correos de forma anónima, y algunas funciones rápidas, como la respuesta automática o el acuse de recibo.

2.2.2. Cifrado

El aspecto más importante, puesto que es el que da un mayor valor diferencial al proyecto, es la seguridad. Por ello, se merece un apartado diferente al que, por organización, podría ser incluido, que es el apartado de Requisitos funcionales.

En el subcapítulo "2.1. La Idea original", tenemos una introducción a los sistemas de criptografía asimétrica. A continuación, vamos a ver el diseño de los mecanismos de cifrado aplicados al problema concreto.

Uno de los modelos de cifrado disponibles más extendido y seguro, que incluso parece que se resiste a la mismísima NSA [10], es *Pretty Good Privacy* (PGP). Este criptosistema incluye elementos de criptografía simétrica y asimétrica.

Vamos a descomponer los pasos del cifrado con PGP:

NOTA: suponemos que los usuarios tienen sendos pares de claves (una pública y otra privada), y las claves públicas son conocidas entre ellos.

1. Tenemos el mensaje en claro, y una clave de sesión generada de forma aleatoria *ad hoc*.
2. El mensaje en claro se cifra con la clave de sesión, utilizando un algoritmo de criptografía simétrica (por ejemplo, AES [11]), obteniendo un mensaje cifrado.
3. La clave de sesión se cifra con la clave pública del destinatario (típicamente, utilizando RSA [12]), obteniendo una clave de sesión cifrada.
4. Se une el mensaje cifrado con la clave de sesión cifrada, y se envía como un único mensaje al receptor.

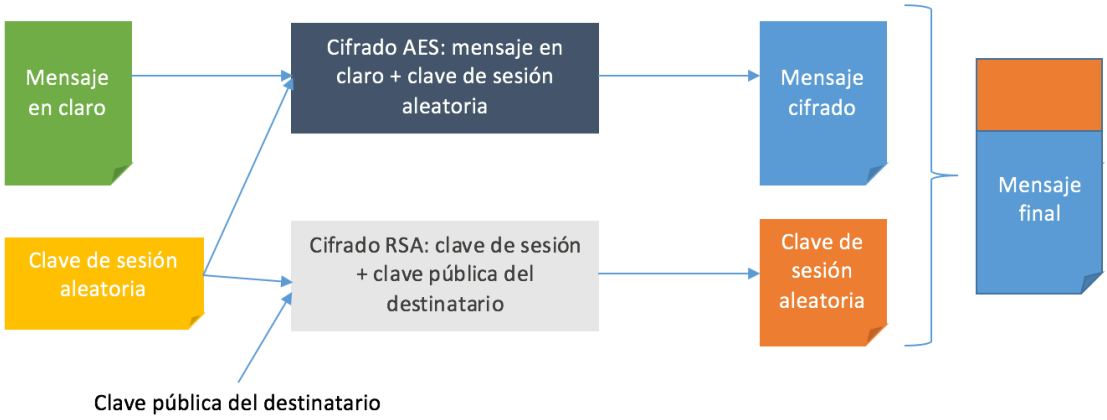

Figura 2.3. Esquema de cifrado en PGP.

10. http://www.theverge.com/2014/12/28/7458159/encryption-standards-the-nsa-cant-crack-pgp-tor-otr-snowden
11. AES: Advanced Encryption Standard. Sistema de cifrado de clave secreta (criptografía simétrica).
12. RSA: Criptosistema de clave pública.

Como resultado final del criptosistema, obtenemos un mensaje que incluye el mensaje original cifrado con una clave de sesión, y la clave de sesión cifrada con la clave pública del receptor. Como hemos comentado anteriormente, exponiendo los fundamentos de la criptografía asimétrica, la clave de sesión, al estar cifrada con la clave pública del receptor, sólo puede ser descifrada con la clave privada del receptor, la cual puede (debe) ser obtenida exclusivamente por el receptor. Esto significa, en teoría, que el único capaz de descifrar la clave de sesión es el receptor. Una vez descifrada dicha clave, la puede usar para descifrar el contenido del mensaje original.

Figura 2.4. Esquema de descifrado en PGP.

Puede notar el lector que, puesto que se utiliza criptografía de clave pública (RSA), para cifrar la llamada clave de sesión, se podría evitar el uso de dicha clave, cifrando directamente el contenido del mensaje con la clave pública del destinatario.

Esto es técnicamente correcto, funcionaría presumiblemente bien y se evitaría tener que generar claves aleatorias de sesión. Sin embargo, ¿por qué se hace de otro modo?

La respuesta corta: por rendimiento. La respuesta larga requiere algo más de explicación.

La seguridad de la criptografía asimétrica, y en concreto RSA, se basa en problemas matemáticos muy complejos de resolver, en términos computacionales.

Si nos fijamos en RSA, su seguridad reside en el problema de la factorización de números enteros. Computacionalmente, podemos calcular el producto (n) de dos números primos (p y q) sin demasiados problemas ($n = pq$), aunque se trate de números considerablemente grandes.

El problema está en descubrir los factores (p y q), conociendo exclusivamente el resultado del producto (n), cuando estos factores son números lo suficientemente grandes (del orden de entre 270 y 617 dígitos decimales), y escogidos al azar.

Este hecho obliga a utilizar claves de entre 896 y 2048 bits (aunque se recomienda utilizar claves de no menos de 1024 bits). Si comparamos el tamaño de estas claves, con el de las de los algoritmos de criptografía simétrica, como AES, cuyo estándar más elevado cuenta con claves de 256 bits, vemos que el tamaño de las primeras es casi 10 veces el de las segundas. Si a esto añadimos que los sistemas de cifrado simétrico suelen ser mucho más rápidos y consumen menos memoria que los asimétricos [13], puesto que éstos requieren un mayor número de cálculos matemáticos, tenemos que el rendimiento de un cifrado simétrico es previsiblemente mayor.

Por ello, buscando optimizar el tiempo necesario para cifrar los correos, que en algunos casos pueden tener longitudes notables, se apuesta por un sistema híbrido basado en PGP.

2.2.3. Modelo conceptual

La idea es, de alguna forma, universalizar el uso de la plataforma. Esta premisa, nos obliga a dar una solución para la inmensa mayoría de sistemas y usuarios. Si optamos por la vía de las aplicaciones nativas, tanto de escritorio como móvil, podríamos hacer un uso intensivo de los sistemas, pero a cambio de varios desarrollos, uno por cada una de ellas (Windows, Linux, MacOS, iOS, Android, …), lo que introduce muchísima más carga de trabajo, con el consiguiente aumento en el consumo de recursos y, por tanto, de presupuesto.

La alternativa que se nos abre, pues, es la de un sistema de computación en la nube. Desarrollando un sistema con un modelo cliente-servidor, con una interfaz de uso en forma de aplicación web, accesible por tanto desde cualquier dispositivo con un navegador, resolviendo así el problema de la compatibilidad entre diferentes

13. Seth, S.M. y Mishra, R. (2011). *Comparative Analysis Of Encryption Algorithms For Data Communication*. http://www.ijcst.com/vol22/2/shashi.pdf

plataformas; nos aprovechamos de la cualidad multiplataforma inherente a este esquema. Este cliente debe incluir todos los requisitos propios de cualquier sistema de sus mismas características (enviar y recibir mensajes, soporte para diferentes buzones, etc.).

La idoneidad de permitir configurar cuentas ya existentes es especialmente importante para las instituciones o empresas que quieran utilizar el sistema. Un usuario particular, que use normalmente su correo Gmail o Hotmail, no tendría un problema demasiado grande en crear una cuenta de correo específico para el correo seguro, siempre y cuando este le interesase lo suficiente. Pero en el caso de una organización, es impensable tener que crear nuevas cuentas para todos los miembros de la misma, máxime cuando se quiere mantener una imagen de marca y una credibilidad coherente con su organización.

La finalidad de la inclusión de la posibilidad de configurar varias cuentas de correo de forma simultánea es ofrecer un cliente de correo web multicuenta, con lo que podemos atraer usuarios no tan interesados en la privacidad, pero sí en la comodidad y la flexibilidad que se brinda al poder acceder a todas tus cuentas en cualquier dispositivo y lugar, sin necesidad de ninguna instalación: simplemente haciendo uso del navegador de internet.

Este hecho permite hacer, de alguna forma, una diferenciación entre dos productos dentro del mismo proyecto. Específicamente, estamos hablando de un cliente web de correo electrónico (webmail), multicuenta y moderno, por un lado; y de un sistema de cifrado y descifrado de correos electrónicos, por otro.

Juntos, forman una solución integral al problema del envío y la recepción de email seguro, permitiendo proteger las comunicaciones de todas las cuentas de correo que estén relacionadas y configuradas por el usuario, con un alto componente de movilidad.

A pesar del planteamiento de desarrollo inicial, en el que se considera únicamente la aplicación web, sería interesante la inclusión de aplicaciones móviles nativas para los sistemas operativos móviles más comunes, como son iOS, Android y Windows 10, en el futuro. Esto se justifica en el potencial de mayor rendimiento que se puede obtener de las aplicaciones nativas (más cuando existen operaciones como es el cifrado y el descifrado, que son bastante complejas), y se llevaría a cabo una vez desplegado el

sistema inicial y obtenida financiación suficiente. Por tanto, y debido al alcance del Trabajo, el desarrollo de aplicaciones nativas queda fuera del mismo.

2.2.4. Diseño y desarrollo del servidor

Para dotar al proyecto del mayor potencial de rendimiento, escalabilidad y elasticidad, se opta por una arquitectura que incluye una base de datos no relacional, MongoDB.

Debido a la experiencia del equipo de desarrollo en tecnologías JavaScript en la parte servidor, además de su idoneidad para entornos con necesidad de ser altamente escalables y modularizables, se selecciona como entorno de desarrollo para el *core* del servidor Node.js [14].

Siguiendo la línea de mantener las mayores capacidades de escalabilidad y modularidad, se diseña y desarrolla una interfaz de programación de aplicaciones (API, por sus siglas en inglés), que permite abstraerse del cliente final, ya sea en forma de aplicación web o aplicación móvil. Para el desarrollo de la API, se hace uso del framework web minimalista para Node.js, Express [15].

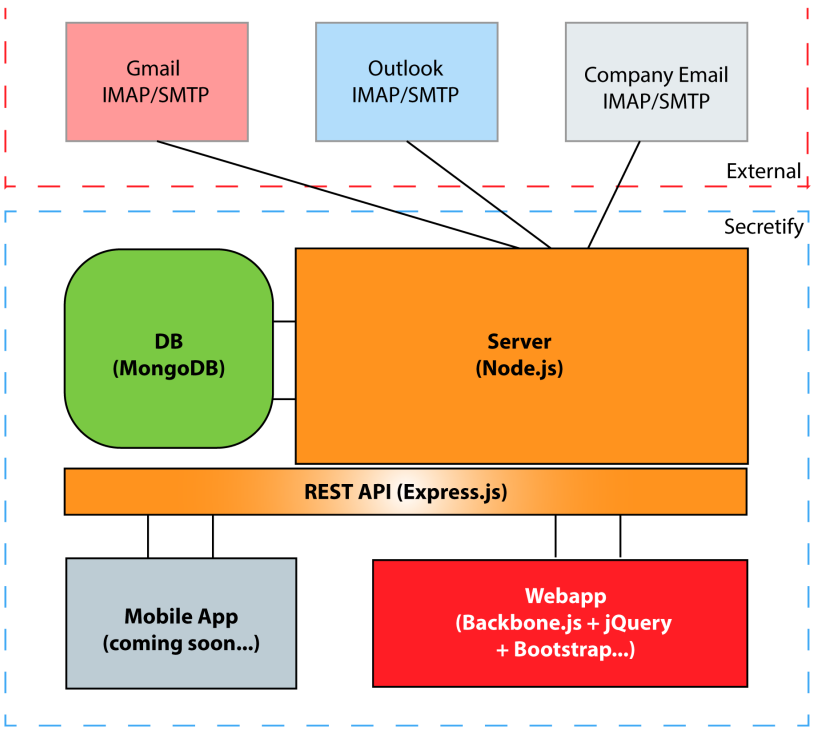

Figura 2.5. Esquema de la arquitectura de Secretify.

14. Node.js. https://nodejs.org/
15. Express. http://expressjs.com/es/

El servidor será el encargado de la comunicación (tanto en el envío como en la recepción de mensajes), con los proveedores de correo del usuario y el almacenamiento y gestión de las claves de forma segura.

Para evitar que nadie tenga acceso al contenido de los mensajes, y puesto que dichos mensajes se envían desde nuestro servidor, el cifrado de los correos electrónicos se va a realizar en el cliente (ya sea aplicación web, móvil, etc). Este esquema de cifrado *end-to-end* (punto a punto), establece que el mensaje se cifra en el cliente del remitente y se descifra en el cliente del destinatario. Por tanto, cualquier paso intermedio, ya sea nuestro servidor, el servidor de correo del proveedor (Gmail, Outlook, Yahoo! Mail, etc.), sólo podrá acceder al email cifrado, y por tanto, ininteligible.

Este hecho facilita la seguridad en el tratamiento de información en el servidor, puesto que ya llega cifrada, pero obliga a implementar mecanismos de seguridad extra en el cliente, para asegurar que no hay vulnerabilidades conocidas en dicho cliente (que no se haya inyectado código malicioso, que el cliente esté autentificado, etc.).

Por otro lado, en cuanto a la gestión de claves, hemos comentado que todas las claves de los usuarios (tanto públicas como privadas), se van a almacenar en nuestras bases de datos. Para mantener la coherencia con nuestra filosofía de acceso nulo a la información, tenemos que desarrollar una política de seguridad al respecto, ya que si estas claves privadas son accesibles por nuestra parte, no tendríamos ningún obstáculo para acceder al contenido de los correos. ¿Cómo garantizamos el no acceso? Cifrando la clave privada de los usuarios con la contraseña de acceso de los usuarios. Para evitar almacenar y conocer la clave de acceso de los usuarios, lo que se almacena para la autenticación es un resumen (*hash*), de la contraseña. Así, en la autenticación, se comparan los *hashes,* uno generado por el cliente al iniciar sesión en el cliente y otro, el almacenado en la base de datos.

Cuando un usuario quiere descifrar un correo electrónico, pide al servidor su clave privada, la cual es devuelta al cliente tal como se almacena en el servidor, cifrada. El usuario, cuando la recibe, la descifra con su contraseña de acceso, que no sale del cliente. Así, obtiene la clave privada y puede utilizarla para el descifrado de mensajes.

Este esquema, además de la seguridad en diseño que provee, tiene una ventaja adicional. Y es que no se depende de una sola clave de aplicación, sino que cada usuario está protegido de forma individual por su clave. Esto hace que si la seguridad de uno de los usuarios se halla comprometida, no se expone a ningún otro usuario. Si por el contrario utilizásemos una clave de aplicación única, por muy larga y segura que fuese, si se ésta llega a comprometerse, todo el sistema estaría expuesto. De la misma manera, al tener desde el servidor un acceso nulo a la información de cifrado de los usuarios, no se expondría información de ningún usuario si se llevase a cabo con éxito un ataque al servidor.

Esto hace que los usuarios no tienen por qué fiarse de nosotros como proveedores de un servicio de cifrado, puesto que ni siquiera nosotros tenemos acceso a sus datos cifrados.

Cabe destacar dentro de este apartado, por último, que para la interacción con los servidores de correo electrónico de los usuarios, se utilizan los protocolos *Internet Message Access Protocol* (IMAP) y *Simple Mail Transfer Protocol* (SMTP), para la recepción y el envío, respectivamente. Esta comunicación se realiza, siempre que el proveedor lo permite, a través de un canal seguro SSL/TLS [16]. Esto es irrelevante para los correos cifrados, porque aunque fuesen interceptados, tendrían que ser descifrados sin ninguna información, pero es importante para los que no están cifrados, ya que se protege su transporte.

2.2.5. Prototipo de la aplicación web

El prototipo realizado del cliente de correo web (webmail), siguiendo la tendencia del servidor, se ha desarrollado utilizando lenguajes y tecnologías sobre JavaScript.

Para la estructura de la aplicación web se ha utilizado el *framework* Backbone.js [17]. Además, en el cliente se hace uso de una de las bibliotecas de código de JavaScript más cómodas y conocidas, jQuery.

En cuanto al diseño, se ha utilizado el archiconocido *framework* de diseño web Bootstrap, y como lenguaje de marcado de plantillas de las vistas de la aplicación, Handlebars [18], que está basado en Mustache [19]. Se ha llevado a cabo un diseño *responsive*, que se adapta al dispositivo y optimiza el tamaño de los elementos para hacerlos accesibles y usables en cualquier smartphone, tablet u ordenador.

16. Transport Layer Security. http://es.wikipedia.org/wiki/Transport_Layer_Security
17. Backbone.js. http://backbonejs.org/
18. Handlebars. http://handlebarsjs.com/
19. Mustache. http://mustache.github.io/

El prototipo, actualmente, permite el envío y la recepción de correo electrónico, tanto cifrado como no cifrado, a excepción de los documentos y archivos adjuntos, siempre y cuando estos no sean imágenes embebidas en el mensaje (que sí se soportan).

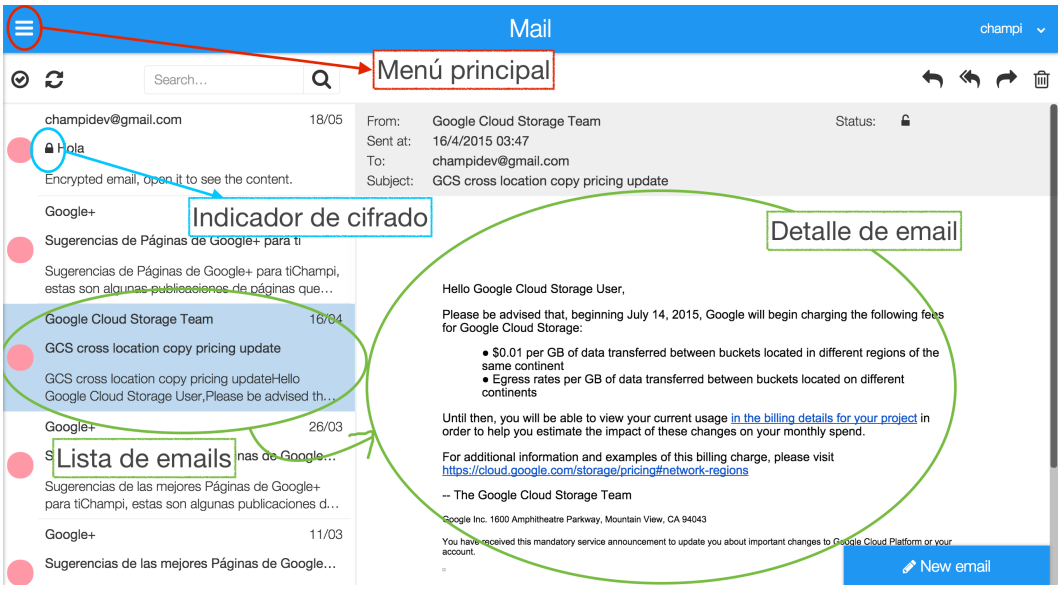

Figura 2.6. Pantalla principal del cliente de correo web, con indicaciones.

Se pueden configurar múltiples cuentas (con un máximo establecido de 3), cada una estará identificada con un color.

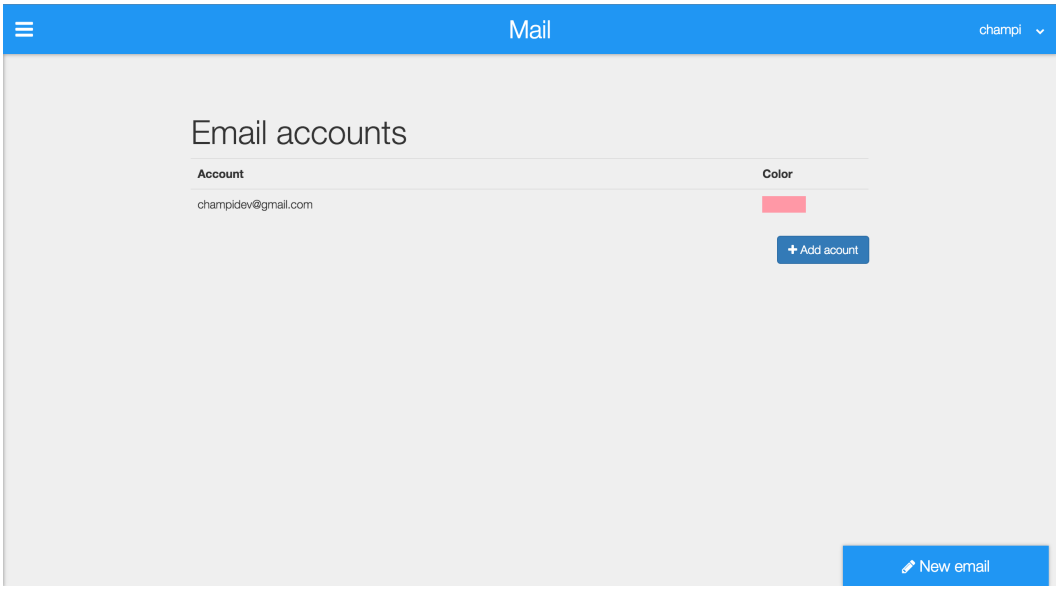

Figura 2.7. Pantalla de ajustes, donde se puede incluir nuevas cuentas de correo.

El usuario puede acceder a los buzones de Recibidos, Enviados, Spam y Papelera.

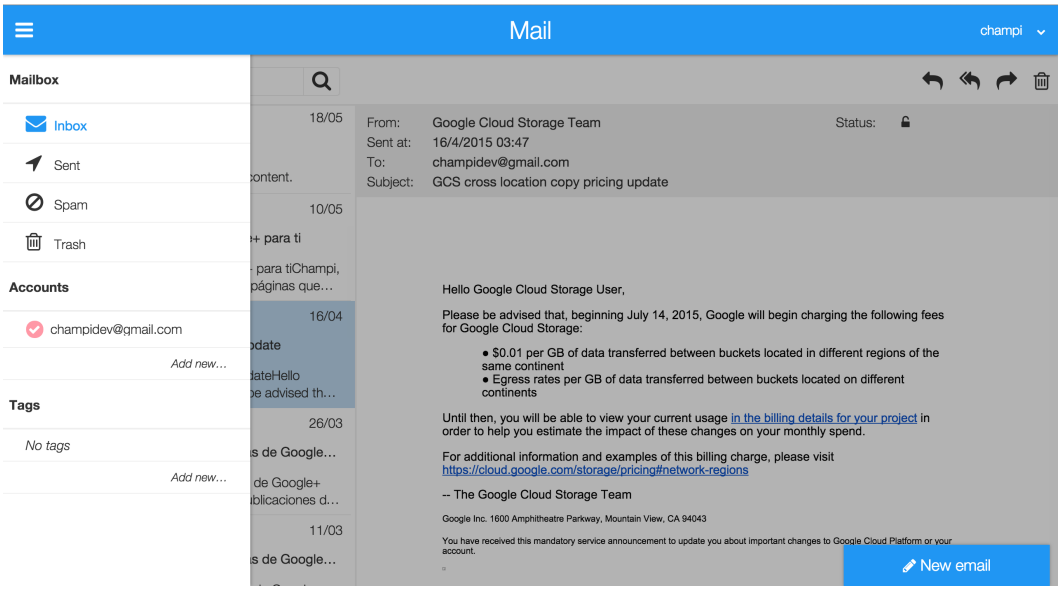

Figura 2.8. Pantalla principal, con el detalle del menú abierto.

En cuanto al envío de mensajes, el sistema es capaz de detectar si los destinatarios están registrados o no en la plataforma, indicándolo con un código de color. Aunque un usuario no esté registrado, se le puede enviar correos cifrados. Para acceder a ellos, debe introducir una clave que se le provee en el primero de estos. Una vez introducido, tiene que crear una contraseña de acceso. Hecho esto, el usuario puede acceder al sistema con la contraseña escogida, y puede leer los correos cifrados recibidos. Para poder enviar debe configurar una cuenta ya existente.

El prototipo de la aplicación está en fase de beta privada.

2.3. De proyecto a producto

Una de las diferencias entre un proyecto y un producto es que, en general, éste debe ser rentable. Esta perspectiva obliga a tomar decisiones y atender a aspectos, que quizás estarían muy por debajo en la lista de prioridades de un proyecto no comercial.

Y uno de los aspectos más importantes hoy en día en los sistemas informáticos, es el visual. Y no es simplemente la usabilidad y la accesibilidad de la aplicación, sino la parte estética, que muchas veces los ingenieros dejamos a un lado.

Esto, que antes quizás podíamos permitírnoslo, hoy ya no es así. Los usuarios instalan y eliminan aplicaciones en cuestión de minutos. El usuario tecnológico medio de nuestros días está acostumbrado a aceptar o descartar una aplicación por su aspecto, si le es atractivo o no, y, para tratar de conseguir y retener el mayor número de usuarios, la parte estética debe ser clave.

Para ello, lo ideal es un aspecto minimalista, con las funciones básicas y más utilizadas al alcance de un click o dos, con elementos visuales claros y bien diferenciados, pero integrados para dar una experiencia de usuario lo más satisfactoria posible. La paleta de colores debe ser también suave y agradable, con una colección de iconos minimalista y elegante.

Uno de los problemas a los que se enfrentan las *startups* es a la falta de financiación. Incluso una vez obtenida, suele ser escasa. Por ello, para evitar desembolsos iniciales demasiado abultados, se toma la decisión de utilizar un esquema de pago por uso para la infraestructura, en concreto, una plataforma como servicio (PaaS). Este modelo permite pagar en función de los recursos que utilizamos y necesitamos, optimizando el gasto.

La consideración más importante, y por lo que un producto o servicio se lanza al mercado, es porque resuelve un problema o una necesidad a una serie personas, a un mercado. Si no hay mercado, no existe un producto. Por ello, es vital identificar a los potenciales usuarios y comprobar las expectativas e interés que el proyecto despierta en ellos.

Capítulo 3. Estrategia

3.1. Mercado

Como hemos comentado anteriormente, el mercado es un aspecto esencial para que un proyecto se convierta en un producto o servicio comercial. Sin un mercado, un producto no se sustenta y desaparece, por lo que no tiene sentido invertir ningún tipo de recurso, ni tiempo ni dinero, a no ser que sepamos y que intuyamos un mercado potencial.

A finales de 2014, según Radicati Group [20], había alrededor de 2.580 millones de usuarios de correo electrónico en el mundo, moviendo más de 205 mil millones de mensajes al día, de los cuales, más de la mitad (112 mil millones), son de ámbito empresarial.

El mercado del correo electrónico es inmensamente grande y tiene un crecimiento esperado del 6% anual, en número de cuentas de correo. Cabe destacar que cada usuario tiene de media 1,7 cuentas de correo electrónico.

3.1.1. Público objetivo

Dentro de esta ingente masa de usuarios, hay muchas personas interesadas y preocupadas por su seguridad; más aún después de las últimas publicaciones en los medios sobre la falta de privacidad que tienen los usuarios de algunos grandes proveedores de servicio, que monitorizan los correos electrónicos, vendiendo o cediendo esa información a terceras partes.

El problema con el sector de los usuarios individuales es que, en general, están acostumbrados a los servicios gratuitos, sin darse cuenta de que realmente están perdiendo privilegios y derechos. Así pues, debemos tener en cuenta que al usuario común no se le puede pedir un precio alto por el servicio.

Por otro lado, tenemos a las empresas, que son más conscientes de la importancia y del valor de la información que manejan y transmiten, y están dispuestas a pagar un mayor precio.

20. Radicati Group. *Email Statistics Report, 2015-2019*. (2015) http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf

En esencia, tenemos como público objetivo, todo aquél usuario individual preocupado por su privacidad, y toda empresa u organización que maneje datos sensibles que merezcan protección.

3.1.2. Primeros pasos

Sin embargo, aún teniendo un mercado potencial gigantesco, no podemos tratar de abarcar todo desde el principio, puesto que nos quedaríamos sin recursos antes de poder alcanzar algún objetivo o trato beneficioso.

Por ello, se destacan nichos o submercados que pueden tener un mayor interés por el servicio de correo seguro.

En primer lugar, aunque más pequeños y con menos capacidad adquisitiva, pero más accesibles, están los bufetes de abogados en general, siendo los que tengan departamentos de derecho Penal o gestión de recursos humanos (que se encarguen de reestructuraciones de personal, etc.), un objetivo más evidente, puesto que gestionan información especialmente sensible dentro de un sector ya de por sí preocupado por la privacidad de las comunicaciones. Estos serían, pues, nuestros primeros objetivos.

Por otro lado, las consultoras medianas y grandes, que tienen servicios de asesoría y consultoría tecnológica, pueden ser excelentes socios y clientes. Clientes, porque pueden incorporar el servicio de correo seguro de forma interna; y socios, porque pueden servir de intermediarios entre nosotros y las empresas dentro de su cartera actual, que puedan precisar de este tipo de servicios de seguridad de la información y las comunicaciones. Aunque a priori esto puede ser más atractivo, es más complicado el acceso y la negociación con este tipo de empresas más grandes.

Cabe destacar dentro de los sectores más sensibilizados o concienciados con la privacidad, podemos contar al Bancario y el de la Salud. Por esta parte, los diferentes bancos o empresas de servicios financieros, o los centros e instituciones sanitarias, pueden estar interesados en integrar el servicio.

Por último, la industria militar, de seguridad tanto del estado como privada, y las agencias de inteligencia o vigilancia, es un campo a tener en cuenta, pero donde es mucho más difícil irrumpir con éxito.

3.2. Modelo de negocio

Como hemos comentado anteriormente, nuestra propuesta de valor es clara: una solución completa e integral para el correo electrónico seguro.

Los potenciales clientes a los que nos dirigimos son los usuarios individuales concienciados con la seguridad de la información y las empresas que manejan datos sensibles que quieren proteger sus comunicaciones a través de correo electrónico.

Además, forma parte de nuestra política ofrecer un servicio asequible a cualquier persona. Teniendo en cuenta que existen dos perfiles muy diferenciados de clientes, es lógico tener una oferta distinta para cada uno de ellos.

Por un lado, para los usuarios individuales, se ofrecerá un servicio totalmente gratuito, con el fin de alcanzar grandes masas de usuarios, y romper la barrera de entrada de los mismos.

Por el otro, ofreceremos unas cuentas, llamadas “corporativas”, que incluyen una serie de servicios adicionales a la capa gratuita, pero con un coste de alrededor de 3 € por usuario al mes (36 € al año por usuario). Este precio viene condicionado, especialmente, por dos factores. Uno de ellos es el precio que tienen servicios como Google Apps for Work, de 4 € por usuario al mes. Queremos que nuestro servicio se pueda montar como una capa extra de seguridad sobre proveedores como Google, por lo que nuestro precio, sumado al del proveedor, no puede ser disparatado. El segundo factor tiene que ver con la filosofía de hacer la seguridad algo accesible. Por ello, y con la intención de captar grandes cantidades de usuarios, queremos que el precio se mantenga lo más asequible posible.

En resumen, nuestro modelo de negocio se basa en un modelo de suscripción *freemium* (incluye una capa de servicios gratuita y otra de pago), sin compromiso de permanencia. La idea es ofrecer una prueba gratuita de 15 o 30 días de la versión de pago, para

mostrar sus funciones avanzadas al usuario, sin obligar a introducir información de pago durante la evaluación.

3.3. Plan de marketing

3.3.1. Objetivo

El objetivo principal del plan de marketing preliminar, es el de conseguir una masa crítica de usuarios. Esto es que en al cabo de los tres primeros meses desde el lanzamiento del servicio, queremos conseguir 1.600 usuarios activos en la plataforma, que luego den pie a una rápida expansión.

Para conseguirlo, tenemos que tener en cuenta diferentes aspectos de la empresa y su relación con los clientes. Desde la imagen corporativa, hasta la publicidad, pasando por el posicionamiento web y el *networking* y presentaciones comerciales en persona.

3.3.2. Imagen corporativa

Durante el Trabajo, hemos ido esbozando la imagen que queremos presentar. Esta es la de una empresa moderna, innovadora y concienciada con la privacidad y la seguridad, pero a la vez divertida.

En base a esto, se ha diseñado un logotipo corporativo, que incluye círculos de colores vivos (azul, verde, naranja, rojo y gris claro), formando la "g" inicial de "guayota studios".

Figura 3.1. Logotipo corporativo.

Para tratar de consolidar una imagen de marca global, se pretende utilizar el nombre principal de la marca, Guayota, para identificar los productos y servicios de la compañía. Así, se plantea que Secretify se convierta en Mail (from Guayota).

Con esta imagen, se pretende dar cabida a un público joven, acostumbrado a la utilización de aplicaciones y herramientas en internet.

3.3.3. Publicidad y posicionamiento

La publicidad, en especial durante los inicios, será la plataforma de dar a conocer un producto novedoso. La intención es poder llegar a los potenciales clientes, para que al menos, conozcan el servicio y la marca. Ir creando un *hype* mediático en todos los usuarios interesados por la seguridad de la información.

En primer lugar, la publicidad irá dirigida a profesionales de la información, seguridad y empresas. La idea es poder presentar el proyecto en foros y grupos de discusión relacionados con la privacidad y la seguridad, en español y en inglés.

En cuanto a los medios gratuitos que se pueden utilizar, se encuentran los perfiles en las redes sociales, como Twitter o Facebook, así como una página web (*landing page*), donde se colgará toda la información con respecto a Secretify.

Por otro lado, se llevarán a cabo campañas de pago, con anuncios en Facebook y en Google (AdWords).

Por último, se utilizarán herramientas de "email marketing" y de "telemarketing", el primero de ellos utilizando una de las plataformas más extendidas para el envío de publicidad a través de correo electrónico, Mailchimp; y el segundo para el contacto con potenciales clientes a través de teléfono. Como se ha comentado en el apartado "3.1.1. Público objetivo", se contactará en un primer momento con empresas que, a priori, puedan estar interesadas en el servicio, como consultoras tecnológicas, banca, despachos de abogados, servicios de la salud y administración pública..

3.3.4. Comercial

Aún con toda la publicidad y el posicionamiento en internet, no debemos olvidar la acción comercial presencial, las redes de contactos personales y profesionales, y las visitas y presentaciones cara a cara.

Durante las primeras etapas, serán los fundadores y promotores del proyecto quienes tomen el papel de embajadores de la empresa y del servicio.

Para comenzar, se pretende llegar a acuerdos de presentaciones y pilotos con empresas e instituciones públicas.

Por otro lado, para favorecer la entrada de clientes que quieran una seguridad en sus pagos o que incluso no quieran dar a conocer su identidad y que no se les pueda trazar a través de cuentas bancarias o los diferentes rastros que deja el dinero, se permitirá realizar pagos a través de plataformas como "Paypal" o algunas de recarga, como "paysafecard".

3.4. Internacionalización

Este proyecto nace con un espíritu internacional. La privacidad y la seguridad de la información es transversal a todos los sectores y organizaciones, y es independiente a la zona geográfica: es necesario en cualquier lugar del mundo.

Además, el modelo de negocio está orientado hacia, y su éxito radica en, un uso masivo de la plataforma. Este proyecto sólo puede ser rentable si se consigue un ingente número de usuarios.

La idea es utilizar el mercado español como experimento y prueba piloto. A la vez, el servicio gratuito estará disponible para los usuarios internacionales, estará traducido a los idiomas más utilizados y se ofrecerá soporte por correo electrónico, al menos, en español e inglés.

Sin embargo, el servicio de pago puede encontrarse con peculiaridades en cuanto a impuestos o tarifas de cambio de moneda, por lo que se debe realizar de forma paulatina, ampliando los países disponibles de forma controlada.

En ambos casos, hay que tener en cuenta la legislación vigente, y estudiar las posibles consecuencias legales de un servicio de estas características, puesto que se tratan temas de seguridad informática, que pueden ser sensibles en algunos países (no es lo mismo que utilice el servicio alguien en un país europeo que alguien en un estado considerado hostil).

La expansión internacional, con apertura de oficinas permanentes en otros países, no se contempla en un principio. Para trabajar con empresas de otros países, se seguirá la máxima de "proveedores globales, *partners* locales". Así, nos podremos aprovechar de una economía de escala, concentrando los gastos en unos pocos proveedores globales, pero contando con la experiencia y el conocimiento de las empresas locales, algo extremadamente importante cuando se trata de un mercado desconocido en un país diferente.

En resumen, en las primeras etapas no realizaríamos una internacionalización propiamente dicha, estando presentes en otros países, abriendo oficinas comerciales y demás. Sino que trataríamos de llegar a acuerdos, en los casos que nos pueda ser interesantes, con socios locales que hagan de intermediarios.

Esto nos permite ser cuidadosos con el dinero, no asumiendo grandes riesgos, pero abriendo la puerta a potenciales socios y clientes del exterior.

A su vez, desde el nacimiento, se construirán los mecanismos que permitan la internacionalización del servicio en cuanto a idiomas, condiciones legales y aceptación de dinero en otras divisas además del euro (al menos, en dólares estadounidenses).

Capítulo 4. Del dinero

4.1. Previsiones: ingresos

Las partidas de ingresos más importantes vendrán dadas por tres elementos.

- Suscripciones de servicio.
- Comisiones o cobros por certificación.
- Soluciones individuales para empresas.

Como hemos comentado en el modelo de negocio, la forma típica de vender el servicio a los clientes es a través de una suscripción mensual. Ésta será la fuente de ingresos más abultada en el futuro, pero, al igual que una cosecha, no obtendremos más que gastos derivados al principio.

Como alternativa de ingresos, planteamos la posibilidad de desarrollar soluciones a medida para las empresas, en *clouds* privadas o sobre sus servidores ya existentes. Estas soluciones a medida mantendrán el núcleo Secretify, pero adaptándose a las condiciones especiales de estas empresas.

Por otro lado, un elemento interesante, es la de la "Certificación" de empresas. En Secretify, nosotros haremos de Autoridad Certificadora, y expediremos los certificados digitales necesarios para el cifrado y el firmado de las comunicaciones. Puede ser interesante para las empresas que formen parte del ecosistema, demostrar su identidad, para evitar fraudes o suplantaciones. Nosotros, como Autoridad dentro de nuestro sistema, seremos quienes nos encargaríamos de comprobar las identidades de los usuarios, ofreciendo un sello de verificación. El ingreso de esta certificación dependerá del tamaño de la empresa, número de usuarios dentro de la plataforma y su volumen de mensajes.

Cabe destacar, aunque estrictamente no forme parte del proyecto, que el equipo empresarial ofrecerá servicios de consultoría tecnológica y desarrollos menores que den una base de ingresos para soportar el proyecto en sus primeros tiempos.

Todas estas fuentes de ingresos están orientadas a mantener activos los servicios garantizando su independencia y estabilidad, sin tener que depender de subvenciones estatales o campañas de donaciones (como Wikipedia). Por otro, lado se pretende dejar fuera todo tipo de publicidad a no ser que fuese necesario para la supervivencias del servicio. Por ello, si lo exige la situación, se introducirá publicidad dentro de la aplicación.

Para el cálculo de las previsiones de ingresos, tenemos que prever el número de usuarios que utilizarán la plataforma. Para ello, vamos a tomar de referencia algunos datos que, aunque no nos permitan pronosticar los ingresos de forma rigurosa, sí nos dan una medida del tamaño del mercado y su potencial.

Como comentábamos en el apartado "3.1. Mercado", y según la fuente ahí mencionada, actualmente hay alrededor de 2,6 mil millones de usuarios de correo electrónico en todo el mundo, de los cuales unos 900 millones son usuarios empresariales. En España [21], tenemos 3,1 millones de empresas, aproximadamente, de las cuales algo más de la mitad son microempresas sin asalariados (en su mayoría autónomos), llegando al 95,8% del total si les sumamos las microempresas con entre 1 y 9 empleados. El 99,88% del tejido empresarial en España está formado por pequeñas y medianas empresas (hasta 249 empleados).

Esta distribución, bastante similar a la media europea (las microempresas constituyen el 92,4% del total frente al 95,8% español), nos brinda un mercado perfecto para Secretify: muchos usuarios diferentes, que buscan servicios útiles y baratos. Queremos aprovecharnos del *long-tail* [22].

Para la realización de las previsiones, suponemos que los gastos comienzan en enero de 2015, mientras que el lanzamiento del producto es en octubre del mismo año. Durante los meses anteriores al lanzamiento, se incurre en gastos relativos al desarrollo y la preparación del proyecto para su comercialización. Debemos acotar el alcance de la previsión, así que esta comienza en el mes 1 (enero de 2015), y finaliza en el mes 45 (septiembre de 2018).

En resumen, los ingresos anuales previstos son:

21. Subdirección General de Apoyo a la PYME, Ministerio de Industria. *Retrato de las PYME 2015*. (2015) http://www.ipyme.org/Publicaciones/Retrato_PYME_2015.pdf
22. Long tail. Wikipedia. https://en.wikipedia.org/wiki/Long_tail

Ingresos			
2015	**2016**	**2017**	**2018**
4.360,00 €	528.240,00 €	2.786.777,44 €	4.086.527,94 €

Tabla 4.1. Tabla de resumen de ingresos anuales.

Nótese que los ingresos reflejados en la Tabla 4.1 en 2015 son a partir de octubre (mes de lanzamiento), y los de 2018 son hasta el mes de septiembre (fin de la previsión).

Las previsiones de ingresos en 2015, son tremendamente pobres. Esto es debido a la conjunción de diferentes elementos: su lanzamiento tardío (octubre de 2015) y la lentitud inicial con la que los usuarios comienzan a adoptar una tecnología novedosa. Esta tendencia de adopción la podemos ver ilustrada en la siguiente gráfica.

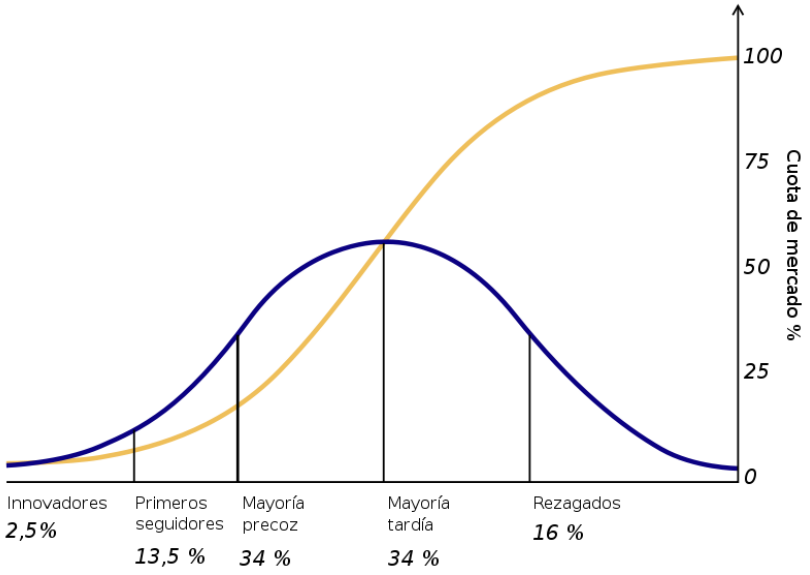

Figura 4.1. Curva de adopción de tecnologías.

Nuestras estimaciones, aún en el caso más optimista, pecan ligeramente de conservadoras. Este hecho ha sido inducido de forma consciente, puesto que preferimos contar y trabajar con los datos más ajustados y pesimistas, dando a entender que aún así hay un negocio detrás de esto.

Cabe destacar que tanto las previsiones de gastos como las de ingresos, no dejan de ser previsiones, y es más plausible que no se cumplan a que lo hagan, pero es un ejercicio

para identificar las fuentes de ingresos y gastos, y así poder anticiparse de alguna forma y prepararse para la realidad.

4.2. Previsiones: gastos

En el caso de los gastos, veremos que los conceptos que más peso tienen varían en función del tiempo. De todas formas, los gastos que a priori se preven son:

- Inversiones (CAPEX).
- Recursos humanos.
- Servicios de pago por uso.
- Marketing, comercial y otros.

En las previsiones de gastos, como norma general, se ha tratado de minimizar, en la medida de lo posible, cualquier salida de dinero. Así pues, se huye de las inversiones en bienes capitales, apostando por una externalización y un modelo de pago por uso.

Por ello, en el apartado de Inversiones o CAPEX (*Capital expenditures*), durante el primer año, sólo se incluirán conceptos relativos a licencias, equipos de desarrollo, mobiliario y otros equipos de oficina, tales como impresoras o teléfonos fijos.

En los primeros meses de desarrollo, antes de contratar personal, los fundadores harán uso de sus propios equipos, para ahorrar costes. A medida que se vaya incorporando gente al equipo, se les irá proveyendo de los equipos necesarios.

Los gastos de inversión que no se podrán evitar al principio, son los de mobiliario y equipos para la oficina. Sin embargo, se pretende hacer uso de instalaciones tales como incubadoras de empresas, que proveen del espacio y la mayor parte del mobiliario (tales como escritorios, sillas y armarios), incluyendo en muchas ocasiones de gastos como luz, agua, limpieza, seguridad e internet, a un precio reducido con respecto al mercado de alquiler. Sólo habría que añadir algunos elementos y equipos de oficina típicos como impresoras o teléfono/fax.

Por otro lado, algunos gastos que tradicionalmente irían a parar al apartado de CAPEX, como pueden ser los servidores con los que dar servicio a los usuarios, se ha decidido que van a pasar a gastos operativos u OPEX (*Operational expenditures*).

Este concepto, si se mantuviese en inversiones, obligaría a adquirir equipos, accesorios y un espacio con los recursos necesarios para dar un servicio con un mínimo de calidad (QoS, *Quality of service*), en cuanto al estado del mismo, y elementos entre los que se incluye la replicación de datos, la protección frente a accesos no autorizados, fuego, inundaciones y desastres naturales, etc.

Esto, que no es más ni menos que la construcción de un centro de procesamiento de datos (CPD), incluye tanto obra civil, como un proyecto de telecomunicaciones, seguridad física y acondicionamiento, dependiendo en gran medida de las infraestructuras de la zona, asumiendo los riesgos que conlleva tener un emplazamiento físico de estas características.

Y por si la inversión necesaria para hacer esto fuera poca, se haría una infrautilización de los servicios que el CPD provee.

Por tanto, en cuanto a la prestación de los servicios, queda totalmente descartada la construcción de un CPD propio. Por ello, tendremos que utilizar instalaciones de terceros. Esto nos deja dos opciones principales: *housing* o *hosting*.

El *housing* es un servicio que ofrecen algunos centros de datos que permite al cliente alojar sus plataformas tecnológicas dentro de las instalaciones del centro. Esto permite a los clientes aprovecharse de la infraestructura y los servicios ya existentes en el entorno del CPD. De alguna forma, se estaría alquilando una parte del centro. Dentro del *housing* existen diferentes modalidades, desde el alquiler de un bastidor o *rack*, en el que instalar un servidor, hasta salas privadas con sistemas de acceso, refrigeración y anti-incendio exclusivos. En cualquiera de las modalidades, haríamos uso de nuestros equipos en la infraestructura alquilada.

Por otro lado, tenemos el *hosting*, donde, a diferencia del *housing*, no tenemos que adquirir equipos informáticos. Simplemente, tenemos que ver qué servicio necesitamos. Estos servicios pueden ir desde el alojamiento de una página web, hasta un servidor dedicado, pasando por los servidores virtuales. Dependiendo de las necesidades del cliente, se puede seleccionar el servicio que más se adecúe. La diferencia está en la capacidad, tanto de cómputo como de almacenamiento, que se ofrece al cliente, con su correspondiente relación de precio.

Dentro del *hosting*, que en este caso podríamos denominar como servicios de computación en la nube o *cloud computing*, existe una estructura que diferencia los servicios en función de su lo que administra el usuario final en contra de lo que administra el proveedor. Dentro de esta estructura, tenemos tres opciones: Infraestructura como servicio (IaaS), Plataforma como servicio (PaaS), y Software como servicio (SaaS) [23].

Nosotros, para dar el servicio, hacemos uso de un PaaS, en concreto, con Heroku [24]. Este proveedor de servicios *cloud*, propiedad de Salesforce, permite desplegar aplicaciones desarrolladas en Ruby, Java, Node.js, Python y PHP, de forma sencilla. Permite incluso, desplegar las aplicaciones desde sistemas de control de versiones, como Git. Este ecosistema facilita la tarea, en gran medida, a los desarrolladores y empresas que quieran desplegar un servicio en internet, puesto que pueden utilizar el lenguaje de desarrollo que prefiera, sin preocuparse de la infraestructura (ni hardware, ni a nivel de sistema operativo, versiones del lenguaje, etc.), ayudándoles a centrarse en el desarrollo y el negocio.

Además, este tipo de plataformas, permiten ir escalando en función de las necesidades. Así, si al principio disponemos de pocos usuarios que no hacen un uso intensivo de nuestro sistema, podremos ahorrar costes de PaaS, puesto que haremos menos uso de plataforma. Si, en cambio, vemos que la demanda de nuestro servicio aumenta, podemos aumentar las necesidades de plataforma sobre la marcha. Existen herramientas que permiten escalar, hacia arriba y hacia abajo, las necesidades en función de la demanda de los usuarios finales, de forma automática. Esto permite economizar y optimar los costes de estructura.

Cabe destacar que el servicio que nosotros ofrecemos, Secretify, es para nuestros clientes un SaaS, que internamente hace uso de un PaaS.

Además de todos los gastos en inversiones y plataforma, tenemos gastos importantes como los de recursos humanos. En concreto, los gastos de personal, equivalen al 46% del total de los gastos del primer año, frente al 1% de los costes de estructura. Con el tiempo, estas proporciones se invierten, siendo en 2018 un 15% del gasto en personal, pasando los costes de estructura a suponer el 62%, a medida que se da servicio a más y más gente.

23. Acens. *El Hosting y la doble A: SaaS, IaaS, PaaS*. (2011). http://www.acens.com/news/septiembre11/WP_acens_el-hosting-y-la-doble-A.pdf
24. Heroku. Portal web. https://www.heroku.com/

La contratación de recursos humanos, al igual que las inversiones, se ha estimado de forma cuidadosa, manteniendo los gastos en los mínimos posibles. Así, durante las primeras etapas del desarrollo, los socios fundadores, con el papel principal de Director General (CEO) y Responsable de Tecnología y Desarrollo (CTO), tendrían que encargarse de la mayoría de los aspectos, desde el desarrollo hasta el marketing, pasando por el soporte a usuarios o la gestión del día a día de la empresa.

A partir de septiembre de 2015, se pretende contratar a dos desarrolladores para que ayuden a finalizar la aplicación, además de llevar a cabo tareas de pruebas. Una vez desplegado el sistema, en noviembre de 2015, se pretende incorporar al equipo a un Ingeniero de Marketing de producto y un Responsable de Ingeniería, que presten apoyo al negocio y promuevan su desarrollo. El equipo se completaría en enero de 2016, incluyendo un Ingeniero de Soporte, que descargaría trabajo a los desarrolladores en la resolución de incidencias técnicas.

Finalmente, además de las inversiones, los gastos de personal y los de pago por uso más importantes, que se refiere a la estructura del servicio, tenemos una serie de gastos menores que hay que tener en cuenta.

En cuanto a la atención a los usuarios, se va a externalizar, de forma que las incidencias o dudas del día a día no requerirá de nuestro tiempo y esfuerzo, sólo llegando a nosotros las más importantes o las que requieran de modificación del sistema.

Por otro lado, se han tenido en cuenta partidas para el alquiler de las oficinas, gastos de marketing, labor comercial y pequeña suma para contingencias.

En resumen, los gastos anuales previstos son:

Gastos			
2015	**2016**	**2017**	**2018**
155.399,12 €	600.795,00 €	995.350,97 €	854.102,99 €

Tabla 4.2. Tabla de resumen de gastos anuales.

4.3. Necesidades de financiación

4.3.1. Resumen

Teniendo en cuenta las previsiones de ingresos y de gastos, podemos hacernos una idea de las necesidades de financiación del proyecto.

La siguiente tabla muestra un resumen de ingresos y gastos anuales previstos:

		2015	2016	2017	2018
Caso teórico	Ingresos	4.360,00 €	528.240,00 €	2.786.777,44 €	4.086.527,94 €
	Gastos	155.399,12 €	600.795,00 €	995.350,97 €	854.102,99 €
Caso optimista	Ingresos	4.796,00 €	571.664,00 €	3.015.439,00 €	4.431.567,00 €
Caso pesimista	Ingresos	3.488,00 €	441.392,00 €	2.329.402,00 €	3.396.408,00 €

Tabla 4.3. Tabla resumen de ingresos y gastos anuales por escenario.

Como vemos, se han tenido en cuenta tres escenarios diferentes. El primero, el teórico, nos servirá de referencia para los supuesto, y para los dos otros dos escenarios: el optimista y el pesimista. El optimista supone una variación de ventas de un 10%, mientras que el pesimista, conlleva una variación de un -20%.

En cualquiera de los casos, durante los dos primeros años, el proyecto arrastraría pérdidas del orden de 150 mil € para el primer año, y de 73 mil € en el segundo. Hay que tener en cuenta que durante el primer año (2015), sólo se obtienen ingresos a partir de octubre, mientras que se acumulan gastos desde enero, una parte de los cuales son virtuales, puesto que entre enero de 2015 y, al menos, julio de 2015, se ha trabajado sin percibir ninguna remuneración, lo que supone un ahorro de al menos 28 mil €. También se pueden reducir costes al principio, no disponiendo de oficina, evitando costes prematuros en marketing o en labor comercial, etc.

Un análisis del flujo de caja previsto nos revela que, hasta el mes 19, julio de 2016, no ingresamos más de lo que gastamos, por lo que es en ese mes en el que mayor descubierto de caja tenemos, situándose en los 303 mill €.

La financiación se suele conceder por años, por lo que es útil un estudio de las necesidades de financiación por cada uno de ellos:

- Para el año 1 (2015), necesitaríamos una financiación de al menos, 150 mil €.
- Para el año 2 (2016), necesitaríamos unos 150 mil € adicionales.
- Durante el año 3 (2017), no necesitaríamos financiación extra, y alcanzaríamos el *payback* en el mes 27 (marzo).

A continuación, se muestra una tabla resumen con los supuestos de flujo de caja y rentabilidad, en función del escenario. Estos escenarios, tal como se ha comentado antes, implican una variación de ventas de un 10% o un -20%, para el caso optimista y pesimista, respectivamente.

	ESCENARIO TEÓRICO	ESCENARIO OPTIMISTA	ESCENARIO PESIMISTA
		% VARIACION VENTAS 10%	% VARIACION VENTAS -20%
Máxima Exposición de Caja	-302.815,46 €	-292.704,46 €	-340.225,46 €
PayBack	27	26	29
VAN (8%)	3.854.475,09 €	4.371.941,57 €	2.819.119,65 €
TIR	11,67%	12,35%	9,99%

Tabla 4.4. Tabla resumen financiero.

Podemos ver que, en cualquiera de los casos, tenemos una rentabilidad, medida con la Tasa Interna de Retorno (TIR), de entre un 10 y un 12%. Este resultado es considerablemente satisfactorio, puesto que a pesar de utilizar datos conservadores, los resultados son atractivos. Entidades como ENISA [25] ofrecen crédito a jóvenes emprendedores al 6%.

No podemos comparar esta rentabilidad con la que ofrece un típico depósito bancario, ya que éste no suele tener un riesgo alto, pero el rendimiento efectivo que se ofrece no va más allá del 2%; o con los bonos del estado, que a 5 años, ofrecen un 1,15%. Sin embargo, tenemos una medida de la rentabilidad sin riesgo. Entra ya dentro de la valoración personal el asumir mayor o menor riesgo en función de la rentabilidad esperada.

25. ENISA - Empresa Nacional de Innovación SA. Portal web. http://www.enisa.es/

4.3.2. Fuentes de financiación

Existen diferentes fuentes de financiación para un proyecto de estas características. A continuación vamos a describir algunos de ellos.

- **Trabajo interno**: la financiación propia más importante es el trabajo de los integrantes del equipo. El tiempo de desarrollo que se emplea y no se remunera, es la partida más rentable de financiación propia. Sin embargo, tiene un límite y es que de algo se tiene que vivir, por lo que no se puede pretender trabajar sin obtener remuneración alguna durante un intervalo de tiempo prolongado. Por otro lado, esto puede funcionar con los fundadores, pero es más complicado convencer a alguien externo: habría que ofrecerle participaciones de la empresa o algún privilegio o bonificación en el futuro.

- **Premios**: ganar premios (sin ceder derechos), en concursos de ideas o emprendimiento, supone una ayuda para la financiación en etapas tempranas. La cuantía de estos premios no suele ser demasiada abultada, pero puede servir como semilla o para promover algo en concreto. En cualquier caso, suponen una inyección de moral, ya que de alguna forma, te están validando la idea.

- ***Business angels***: la inversión por parte de un *privatus*, que entra como socio capitalista de la empresa. Este tipo de inversor trabaja con su propio patrimonio, por lo que suele invertir en etapas tempranas, con un capital (relativamente) reducido, y suele buscar una rentabilidad alta en poco tiempo.

- Las tres "f", ***family, friends & fools***: es una opción interesante cuando las necesidades de financiación no son muy grandes o como punto de partida para el desarrollo. Pedir dinero a amigos y familia siempre conlleva algunos riesgos personales.

- **Capital riesgo**: a los fondos y las entidades de capital riesgo lo único que les interesa es la recuperación de la inversión con la mayor rentabilidad posible. Por tanto, hay que tener cuidado puesto que sus intereses puede que no siempre estén alineados con los del equipo emprendedor. Sin embargo, en algunas ocasiones son la única opción

para una empresa que necesita obtener una financiación considerablemente alto, sin ofrecer suficientes garantías.

- **Préstamos participativos o subvenciones**: préstamos con intereses muy bajos y períodos de carencia del principal largos, o incluso subvenciones a fondo perdido hacen de este tipo de financiación una de las más atractivas, pues suelen ofrecer cuantías elevadas. Por otro lado, son más complicadas de conseguir, estudian a fondo el proyecto y son procesos lentos y tediosos, llenos de presentaciones de documentación. En muchas ocasiones suelen exigir que el proyecto tenga "tracción", esto es, que el proyecto ya tenga clientes, tenga pilotos con empresas y que se vea que existe de verdad un valor en la idea, que se lleva a cabo y que hay clientes.

- **Aceleradoras de empresas**: suelen ofrecer un capital semilla inicial limitado y una mentorización durante el proceso de aceleración. Generalmente, piden a cambio un porcentaje minoritario, de entre un 10 y un 20% de las participaciones, además de la firma de un pacto de socios. En algunas ocasiones, estos pactos de socio suelen imponer condiciones similares a las de las entidades de capital riesgo, aunque ofrecen un décima parte que éstas.

- ***Crowdfunding***: últimamente de moda, es una forma de financiación colectiva a través de micro-financiaciones. Se le llama en ocasiones, micromecenazgo. Hay que tener en cuenta que hay diferentes formas de *crowdfunding*, en función de lo que espera el microinversor al aportar dinero: sin contrapartida alguna, recompensas (tales como *merchandising*, acceso privilegiado, etc.), o micro-participación en la empresa. En España no gozan de una gran popularidad, pero sí a nivel internacional (sobre todo en Estados Unidos). Cabe destacar que hay plataformas, como Kickstarter [26], que no permiten la inclusión de proyectos españoles.

- **Financiación tradicional**: no podemos olvidar las formas de financiación tradicionales, como los créditos o los prestamos bancarios. Esta forma de financiación es complicada hoy en día, puesto que las entidades financieras no suelen ofrecer cuantías elevadas, y aplican tipos de interés alto, que hacen esta financiación poco atractiva.

26. Kickstarter. Portal web. https://www.kickstarter.com/

En general, a pesar de la existencia de múltiples fuentes de financiación, la realidad es que es complicado financiar un proyecto, y más aún cuando no se dispone de un prototipo o una prueba de concepto.

Aún poseyendo un llamado producto mínimo viable (MVP), muchas entidades requieren de la demostración de cierta tracción, para estar seguros de la existencia de clientes y de la validez de la idea y la solución desarrollada. Además, este tipo de procedimientos conlleva la preparación y generación de mucha documentación relacionada con el proyecto, desde previsiones del flujo de caja, hasta pilotos desarrollados o documentación técnica.

Para nuestro proyecto, pretendemos conseguir un capital semilla con aportaciones de los socios y su entorno, sin diluir participaciones. Con ello, se pretende desplegar el producto mínimo viable y obtener pilotos y pruebas con empresas e instituciones, que sirvan para validar el modelo. Una vez hecho esto, se presentarán los resultados a diferentes instituciones públicas que ofrecen préstamos participativos y subvenciones, para acabar en contacto, si es necesario, con entidades de capital riesgo.

Capítulo 5. Plan de negocio

5.1. Introducción

El **Plan de negocio** es el documento de **descripción de un proyecto comercial** por excelencia. Hay un debate generalizado, entre quienes opinan que es una pérdida de tiempo, ya que nunca se cumple, y entre quienes defienden que es un ejercicio de reflexión imprescindible sobre un negocio.

La realidad es que el Plan de negocio es un documento imprescindible cuando se requiere de financiación externa, pues es la forma de un proyecto desconocido y con múltiples incógnitas a un potencial inversor.

El Plan de negocio toca los diferentes aspectos que intervienen, como son el **producto de valor**, el **mercado y la competencia**, el **modelo de negocio**, el **plan financiero**, la **organización**, **marketing y ventas**, potenciales **alianzas** y los **riesgos** a los que se enfrenta el proyecto.

En este capítulo se pretende recapitulación resumen del presente Trabajo con el "Resumen ejecutivo", así como comentar algunos aspectos que han quedado fuera de los capítulos anteriores, como la "Organización empresarial" y los "Riesgos y estrategia de salida".

5.2. Resumen ejecutivo

El resumen ejecutivo del plan de negocio pretende presentar, en una página, la idea principal del proyecto. Es un aspecto esencial, puesto que es lo primero que un potencial inversor se lee y puede marcar la diferencia entre decidirse a profundizar en el plan o descartarlo definitivamente.

El resumen ejecutivo puede estar dividido en los siguientes apartados.

5.2.1. Idea de negocio

Tu correo electrónico ahora es privado, sólo con un click. Desde tu navegador web puedes proteger tus cuentas de correo, unificándolas todas y gestionándolas desde el mismo lugar.

5.2.2. Público objetivo

Todo aquél usuario individual preocupado por su privacidad, y toda empresa que maneje informaciones y comunicaciones sensibles que merezcan protección.

5.2.3. Valor añadido

- Centralización de cuentas, permitiendo una gestión de las comunicaciones más sencilla y directa.
- Implantación de mecanismos robustos de seguridad de la información de forma efectiva y fácil de usar.
- Todo ello sin necesidad de instalar nada, simplemente accediendo al servicio desde un navegador web con conexión a Internet.

5.2.4. Tamaño de mercado

Actualmente, hay más de 2.580 millones de usuarios de correo electrónico, y se espera un crecimiento anual mantenido del 6%.

5.2.3. Entorno competitivo

Existen diferentes alternativas para el cifrado de correos electrónicos, pero ninguna dispone de todas las ventajas que presenta esta solución.

5.2.4. Estado del desarrollo

El prototipo de un producto mínimo viable (MVP), está finalizado. Actualmente se puede gestionar el envío y la recepción de correo normal y seguro.

5.2.5. Inversión

Para la puesta en marcha del proyecto se precisa una primera ronda de financiación de 150.000 €.

5.2.6. Objetivos a medio y largo plazo

El objetivo principal a medio plazo es el de llegar a un gran número de usuarios de correo electrónico conscientes de la precariedad de la seguridad de su información, así como llegar al mayor número de empresas posible, para empezar a realizar pilotos y *betas* con usuarios reales.

A largo plazo, se busca implantar este sistema como un estándar de facto para las comunicaciones seguras dentro del correo electrónico.

5.3. Organización empresarial

Para el desarrollo y la comercialización del proyecto Secretify, se ha constituido una empresa, Guayota Studios SL, fundada por los promotores y desarrolladores de la idea, Urko Martinez y Esaú Suárez. Cada uno de ellos es el encargado de un área específica dentro de la empresa, en función de sus especialidades y preferencias.

Además de ellos, cuentan con la ayuda de diferentes profesionales que se encargan y dan apoyo en aspectos como el diseño, el marketing o la administración de la empresa.

5.4. Riesgos y estrategia de salida

5.4.1. Riesgos

Uno de los grandes riesgos a los que se enfrenta el proyecto es a la todavía **precaria concienciación** por parte de la población de la **falta de privacidad** en las comunicaciones.

Muchas personas no creen que el tema de la privacidad y la seguridad en internet sea importante para ellos. Así pues, podríamos encontrarnos un **mercado no tan maduro** como nos gustaría. Este cambio de mentalidad en la percepción de la seguridad en nuestra vida en internet, requiere de una educación y un conocimiento sobre tema, algo complicado de conseguir.

Sin embargo, nuestro modelo de negocio se basa en las **empresas y en los particulares que ya son conscientes de la importancia de la privacidad**, por lo que nuestros ingresos no se verían afectados por el número de usuarios particulares normales, que harían uso de la versión gratuita de la plataforma. Sin embargo, nuestro objetivo es

convertirnos en en el sinónimo de correo electrónico seguro, por lo que se pretende llevar a cabo campañas y trabajos que promuevan la aplicación de la seguridad en las tecnologías de la información y las comunicaciones (TIC). Es responsabilidad de todos, empresas, instituciones e individuos, facilitar el acceso a los conocimientos, en este caso, sobre la privacidad.

Por otro lado, tenemos en frente la **natural resistencia al cambio**. Nuestra solución implica el uso de una aplicación web para la gestión de los correos electrónicos. Hay muchas empresas y particulares que, a priori, no querrán salir de su ya acostumbrado Outlook, Thunderbird o Gmail.com. Para solventar este escollo, trataremos de ver las ventajas de utilizar su cuentas de correo existentes, en una plataforma pensada para la sencillez de uso, con funciones rápidas que optimizan y mejoran la productividad de los usuarios, y que integran de forma transparente, los más elevados mecanismos de seguridad.

Además, somos un proyecto y una empresa novedosos y desconocidos, lo que puede acarrear **falta de confianza** por parte de los potenciales clientes. Vamos a paliar esta situación y aumentar la confianza de los usuarios llevando a cabo auditorías y certificaciones de organismos reconocidos. Se plantea, en el futuro, abrir parte del código a la comunidad, para que cualquiera pueda comprobar por sí mismo la seguridad de la solución implementada.

Un riesgo, común a la mayoría de este tipo de proyectos, es que el **número de usuarios no aumente tan rápido como se esperaba**. En otros casos, esto podría llevar a situaciones en las que hubiese recursos infrautilizados (como capacidad de cómputo o almacenamiento). Sin embargo, nuestro modelo de pago por uso de la infraestructura que necesitamos, nos permite crecer sin desperdiciar recursos, optimizando nuestras finanzas.

5.4.2. Estrategia de salida

Una de las estrategias de salida más comunes en este tipo de empresas, es la adquisición de la misma por parte de alguna más grande o preponderante en el sector.

Si se diese el caso, las empresas que más interesadas en el proyecto pueden estar son los gigantes del software e internet, como son Microsoft o Google, o más probablemente,

compañías dedicadas a la seguridad de la información, como McAfee (propiedad de Intel), Symantec o Cisco - Security.

Compañías españolas, aunque multinacionales, como Telefónica o Indra, entre otras, tienen divisiones y departamentos dedicados a la seguridad, por lo que, si se demuestra que hay un mercado para la idea y se convierte en un negocio rentable, pueden estar interesadas en una adquisición.

Capítulo 6. Conclusiones y trabajos futuros

6.1. Conclusiones

El presente Trabajo pretende dar un visión general del proceso que va, desde el surgimiento de una idea innovadora, hasta la preparación del lanzamiento de un producto o servicio tecnológico, aplicado a un caso real.

Durante el mismo, hemos ido viendo los pormenores y detalles, desde la problemática que existe alrededor de la privacidad, hasta las dificultades en la búsqueda de financiación.

Por un lado, se ha conseguido dar una solución a cada uno de los objetivos planteados al inicio del Trabajo de forma satisfactoria. En definitiva, se han aplicado los conocimientos adquiridos durante el Máster en la preparación del lanzamiento de un producto tecnológico comercial, desde la definición del producto, hasta la generación del contenido necesario para presentar un Plan de negocio a un inversor.

Por el otro, se ha constituido una sociedad mercantil para el lanzamiento de la plataforma y el desarrollo de la actividad. Se dispone de una versión beta privada, actualmente en pruebas.

6.2. Trabajos futuros

Como trabajos futuros dentro del proyecto tecnológico, se pretende desarrollar una funcionalidad que ha quedado en el tintero, como es la gestión de documentos adjuntos (acutualmente no disponible). Además, sería positivo desarrollar las versiones para aplicaciones móviles.

Por otro lado, se espera sacar una beta pública en los próximos meses, aún sin concretar.

Se han iniciado contactos con diferentes organizaciones para obtener la financiación necesaria para realizar el proyecto.

Bibliografía y referencias

1. Informe Sociedad de la Información en España 2014. 2015. VV.AA. Fundación Telefónica. 3

2. Why startups fail, according to their founders. http://fortune.com/2014/09/25/why-startups-fail-according-to-their-founders/ 4

3. Google: don't expect privacy when sending to Gmail. The Guardian. http://www.theguardian.com/technology/2013/aug/14/google-gmail-users-privacy-email-lawsuit 8

4. Patriot Act. Wikipedia. http://en.wikipedia.org/wiki/Patriot_Act 9

5. Sentencia del TEDH Klass y otros contra Alemania, 1978, y Sentencia del TEDH Leander contra Suecia, 1987. Cita de Rodríguez, O. T. (2014). Seguridad del Estado y privacidad. Editorial Reus. 9

6. Secrets, lies and Snowden's email: why I was forced to shut down Lavabit. The Guardian. http://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email 9

7. Cliente de correo electrónico. Wikipedia. http://es.wikipedia.org/wiki/Cliente_de_correo_electr%C3%B3nico 10

8. Silent Circle. Wikipedia. http://en.wikipedia.org/wiki/Silent_Circle_(software) 12

9. OpenSSL Project web. https://www.openssl.org/ 13

10. http://www.theverge.com/2014/12/28/7458159/encryption-standards-the-nsa-cant-crack-pgp-tor-otr-snowden 17

Este documento esta firmado por

	**Firmante**	CN=tfgm.fi.upm.es, OU=CCFI, O=Facultad de Informatica - UPM, C=ES
	Fecha/Hora	Sat Jun 20 01:48:14 CEST 2015
	Emisor del Certificado	EMAILADDRESS=camanager@fi.upm.es, CN=CA Facultad de Informatica, O=Facultad de Informatica - UPM, C=ES
	Numero de Serie	630
	Metodo	urn:adobe.com:Adobe.PPKLite:adbe.pkcs7.sha1 (Adobe Signature)